



UTPL
La Universidad Católica de Loja

Modalidad Abierta y a Distancia



Fundamentos y Aplicación de Seguridad de la Información

Guía didáctica

Facultad de Ingenierías y Arquitectura

Departamento de Ciencias de la Computación y Electrónica

Fundamentos y Aplicación de Seguridad de la Información

Guía didáctica

Carrera	PAO Nivel
▪ <i>Tecnologías de la información</i>	VIII

Autores:

Romero González Karla Alexandra
Jaramillo Hurtado Danilo Rubén



D S O F _ 4 0 7 7

Asesoría virtual
www.utpl.edu.ec

Fundamentos y Aplicación de Seguridad de la Información

Guía didáctica

Romero González Karla Alexandra
Jaramillo Hurtado Danilo Rubén

Universidad Técnica Particular de Loja



4.0, CC BY-NY-SA

Diagramación y diseño digital:

Ediloja Cía. Ltda.
Telefax: 593-7-2611418.
San Cayetano Alto s/n.
www.ediloja.com.ec
edilojainfo@ediloja.com.ec
Loja-Ecuador

ISBN digital - 978-9942-39-298-5



La versión digital ha sido acreditada bajo la licencia Creative Commons 4.0, CC BY-NY-SA: Reconocimiento-No comercial-Compartir igual; la cual permite: copiar, distribuir y comunicar públicamente la obra, mientras se reconozca la autoría original, no se utilice con fines comerciales y se permiten obras derivadas, siempre que mantenga la misma licencia al ser divulgada. <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es>

30 de septiembre, 2021

Índice

1. Datos de información.....	9
1.1. Presentación de la asignatura	9
1.2. Competencias genéricas de la UTPL	9
1.3. Competencias específicas de la carrera	9
1.4. Problemática que aborda la asignatura.....	10
2. Metodología de aprendizaje.....	11
3. Orientaciones didácticas por resultados de aprendizaje.....	13
Primer bimestre	13
Resultado de aprendizaje 1	13
Contenidos, recursos y actividades de aprendizaje	13
Semana 1	14
Unidad 1. Fundamentos de seguridad de la información	14
1.1. ¿Qué es la seguridad de la información?.....	15
1.2. Objetivos de la seguridad de la información	24
1.3. Definiciones dentro de la seguridad de la información	24
Actividades de aprendizaje recomendadas	27
Resultado de aprendizaje 2 y 3	28
Contenidos, recursos y actividades de aprendizaje	28
Semana 2	28
1.4. Estándares usados para la seguridad de la información	28
1.5. Sistemas de gestión de seguridad de la información SGSI	37
1.6. Auditoría de un Sistema de gestión de seguridad de la información SGSI	41
1.7. Fases de auditoría de un SGSI.....	41
Actividades de aprendizaje recomendadas	44
Autoevaluación 1	46

Resultado de aprendizaje 4.....	48
Contenidos, recursos y actividades de aprendizaje	48
Semana 3	48
Unidad 2. Gestión de riesgos	48
2.1. ¿Qué es la gestión de riesgos?.....	48
2.2. Contexto de la Gestión de Riesgos	52
2.3. Proceso de análisis del riesgo.....	55
2.4. Proceso de evaluación del riesgo	65
Actividades de aprendizaje recomendadas	70
Resultado de aprendizaje 5.....	71
Contenidos, recursos y actividades de aprendizaje	71
Semana 4	71
2.5. Valoración del riesgo – Matriz de riesgo	71
2.6. Proceso de tratamiento de los riesgos	78
2.7. Monitoreo y reportes del riesgo	83
2.8. Marcos metodológicos para la gestión de riesgos.....	85
Actividades de aprendizaje recomendadas	95
Autoevaluación 2	97
Resultado de aprendizaje 6	100
Contenidos, recursos y actividades de aprendizaje	100
Semana 5	100
Unidad 3. Análisis de ataques a los sistemas de información.....	100
3.1. Problemas de seguridad de la información.....	102
3.2. Software en la organización	106
3.3. Seguridad del software	108
3.4. Ataques a los sistemas de información a través de Internet.....	109
3.5. Tendencias de los ataques.....	110
Actividades de aprendizaje recomendadas	111

Semana 6 y 7	114
3.6. Ataques a los sistemas.....	114
3.7. Tipos de ataque a los Sistemas de Información.....	124
Actividades de aprendizaje recomendadas	135
Autoevaluación 3	138
Semana 8	141
Actividades de aprendizaje recomendadas	141
Segundo bimestre	142
Resultado de aprendizaje 6.....	142
Contenidos, recursos y actividades de aprendizaje	142
Semana 9	142
Unidad 4. Desarrollo seguro de aplicaciones.....	142
4.1. Importancia del desarrollo seguro de aplicaciones.....	143
4.2. Requisitos de Seguridad	149
4.3. Diseño Seguro	151
4.4. Codificación Segura	153
4.5. Los touchpoints de seguridad del software durante el ciclo de vida de Sistemas	154
Actividades de aprendizaje recomendadas	157
Semana 10	158
4.6. Seguridad en aplicaciones Web. OWASP	158
4.7. Protección de sitios con protocolo HTTPS	165
4.8. Uso de certificado SSL.....	166
4.9. Control de Acceso	168
Actividades de aprendizaje recomendadas	174
Autoevaluación 4	175

Resultado de aprendizaje 8	178
Contenidos, recursos y actividades de aprendizaje	178
Semana 11	178
Unidad 5. Análisis forense	178
5.1. Análisis forense informático	178
5.2. ¿Qué es y para qué sirve el análisis forense informático?	179
5.3. Tipo de análisis forense.....	180
5.4. Principios del análisis forense.....	180
5.5. Usos de la informática forense	181
5.6. Uso de análisis forense.....	182
5.7. Manejo de incidentes informáticos.....	183
Actividades de aprendizaje recomendadas	185
Semana 12	186
5.8. Metodologías de análisis forenses	186
5.9. Herramientas para análisis forense	189
5.10. Plan de respuesta a incidentes informáticos	191
Actividades de aprendizaje recomendadas	193
Autoevaluación 5	195
Semana 13 y 14.....	198
Unidad 6. Gestión de la continuidad de negocio	198
6.1. ¿Qué es la gestión de continuidad de negocio?.....	198
6.2. Plan de continuidad del negocio	202
Actividades de aprendizaje recomendadas	223
Semana 15	224
6.3. Gestión de incidentes de seguridad - CSIRT.....	224
6.4. Buenas prácticas para la continuidad de negocio	230
Actividades de aprendizaje recomendadas	236
Autoevaluación 6	237

Semana 16	240
Actividades de aprendizaje recomendadas	240
4. Solucionario	241
5. Glosario.....	247
6. Referencias bibliográficas	248
7. Anexos	254



1. Datos de información

1.1. Presentación de la asignatura



1.2. Competencias genéricas de la UTPL

- Comportamiento ético.

1.3. Competencias específicas de la carrera

Asegurar la calidad, tanto de los productos como de los procesos, en los proyectos informáticos, utilizando buenas prácticas definidas por la industria para garantizar sistemas eficientes y negocios rentables.

Implementar mecanismos de seguridad física y lógica en los sistemas organizacionales mediante el uso de estándares y marcos de trabajo internacionales que garanticen la correcta operación del negocio.

1.4. Problemática que aborda la asignatura

- Implementación de seguridad en los sistemas de información basados en buenas prácticas, marcos de referencia o estándares.
- Comprender aspectos fundamentales de la seguridad de la información en todos los niveles de una organización.
- Comprender la importancia del proceso de gestión de riesgos adecuado y el tratamiento de estos riesgos de manera sistemática.
- Comprender la importancia de un plan de continuidad de negocio, sobre todo para restablecer la normalidad de los procesos críticos de la organización interrumpidos por un incidente.
- Conocer los principales ataques a los sistemas de información y cómo defenderse.
- Comprender el ciclo de vida de desarrollo de aplicaciones seguras.
- Utilizar el análisis forense como herramienta para determinar un por qué y de qué manera ocurrió un delito informático o un incidente.
- Definición de un marco para describir cómo una comunidad productiva puede organizarse con el apoyo de las tecnologías de la información para mejorar su producción y oportunidades de negocio.



2. Metodología de aprendizaje

Para el estudio de esta asignatura se utilizará algunas herramientas que le servirán como apoyo para que logre obtener los conocimientos y competencias al finalizar esta materia y que le servirán para aplicar en su vida profesional.

Es importante que para la tutoría usted previamente haya revisado el contenido que está planificado semanalmente y haga la debida interacción con el docente, de tal manera que la tutoría sirva como refuerzo a lo que usted previamente estudió. Así mismo se pide que, en cada tarea enviada o planificada como un componente práctico experimental, lea y comprenda detenidamente qué se solicita que desarrolle, ya que se orientará a que estas tareas sean basadas en análisis de casos de estudio o análisis basados en problemas, en los cuales usted deberá dar una respuesta de un caso o problema en particular, utilizando los conocimientos estudiados y que tiene relación con la solución que se pide del estudio de caso o problema. También es importante que esté atento al plan de estudios para que sepa en qué casos utilizar el Laboratorio Virtual, porque las tareas serán también enfocadas en la parte práctica.

Antes de empezar el estudio de los contenidos de este texto guía es importante que usted lea los siguientes lineamientos y recomendaciones que le ayudarán a que el estudio de la materia sea lo más fácil posible:

- Revise el plan de estudio de la asignatura para que su estudio sea acorde a lo que se ha planificado semanalmente en cuanto a estudio de contenido y también para que tenga en cuenta las actividades ACD (Acompañamiento con el Docente), APE (Aprendizaje Práctico Experimental) y AA (Aprendizaje Autónomo) que debe realizar.
- Ingrese al EVA para que esté pendiente de las fechas de actividades en línea, ya que aquí puede revisar las que están programadas y estar al tanto de la fecha límite de realización de la actividad o de entrega.

- Ingrese al EVA para que revise los anuncios semanales y sobre todo las tutorías grabadas donde se explicará el contenido de la materia por semana. Así mismo habrá anuncios con lineamientos específicos de la asignatura o de estrategias para realizar las tareas.
- Recuerde que las tareas *Aprendizaje Práctico Experimental* debe enviarlas en fechas programadas, las cuales también están en el plan docente y configuradas en el EVA. Es importante que haga una lectura comprensiva de la actividad que debe desarrollar con la finalidad de que sean entregadas a tiempo.
- Por cada unidad de estudio usted tiene actividades recomendadas y aunque no tienen un puntaje dentro del desarrollo de la asignatura, le sirven para afianzar conocimientos y para realizar las APE. Por lo tanto, es importante su compromiso al desarrollarlas.
- Al finalizar el estudio de cada unidad se recomienda desarrollar las autoevaluaciones que estarán configuradas tanto en el EVA como las tendrá expuestas en el texto guía, de tal manera que así puede usted mismo autoevaluarse y darse cuenta de qué puntos de la asignatura debe afianzar más.
- Utilice los diferentes canales de comunicación (correo electrónico, EVA, vía telefónica o chat) para comunicarse con su tutor y exponer sus dudas e inquietudes. No olvide que cada ciclo le es asignado un horario con el día y la hora específica para la tutoría.



3. Orientaciones didácticas por resultados de aprendizaje



Primer bimestre

Resultado de aprendizaje 1

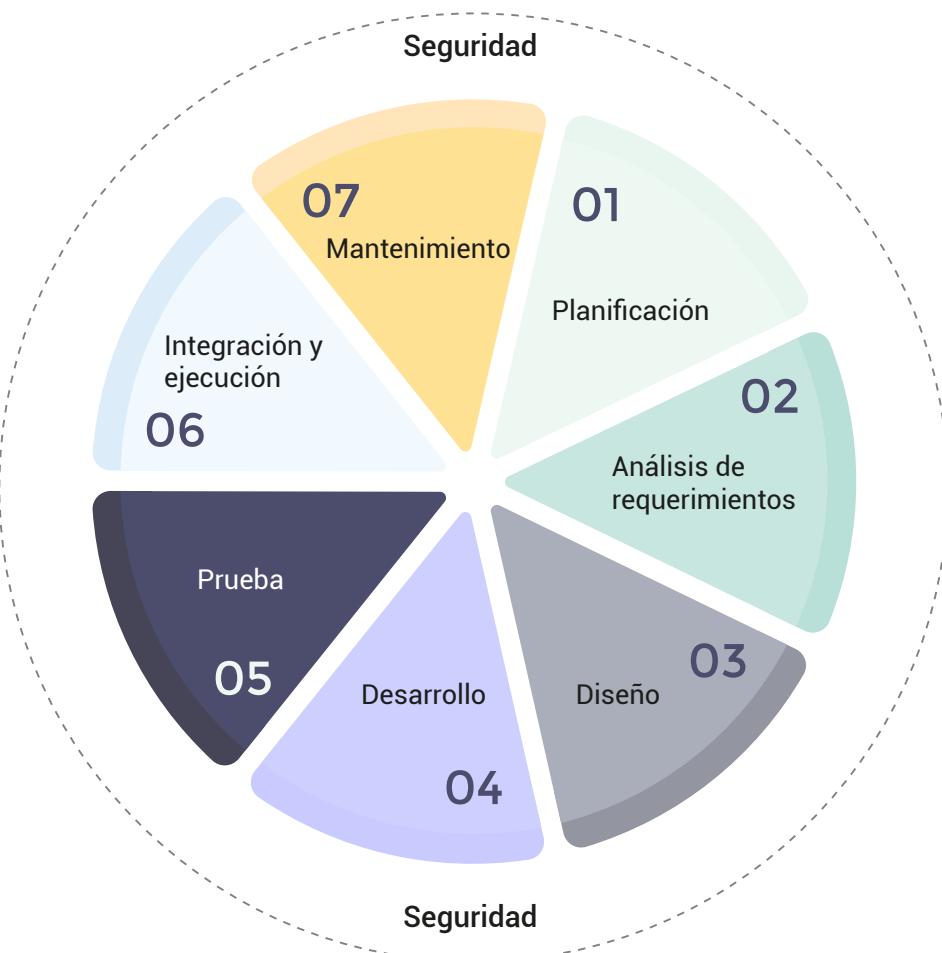
- Fundamentar el porqué del aseguramiento de la información y la seguridad deben ser incluidos como parte del diseño y la arquitectura en el ciclo de vida de sistemas de información.

Contenidos, recursos y actividades de aprendizaje

Estimados estudiantes, seguramente ustedes han escuchado o han sido testigos de ciertos incidentes en algunas organizaciones donde, por ejemplo, sus sistemas informáticos fueron atacados por un *hacker*, donde hubo un incidente de seguridad porque un miembro del personal no tuvo cuidado con la contraseña que usa dentro de la organización e incluso donde por algún motivo hubo un robo de recursos físicos de la organización. Sea cual sea el caso, puede darse cuenta de que esto sucede sobre todo por la falta de controles y contingencia de algún tipo dentro de la organización. Al estudiar esta unidad usted estará en la capacidad de reconocer y diferenciar los conceptos relacionados con la seguridad de la información y entender por qué el proceso de aseguramiento de información es tan importante dentro del ciclo de vida de los sistemas de información de las organizaciones, convirtiéndose en una fase paralela al mismo. En la figura 1 tenemos la seguridad como capa transversal que cubre cada una de las fases del ciclo de vida de un sistema de información.

Figura 1.

Ciclo de vida de un sistema de información y seguridad



Semana 1

Unidad 1. Fundamentos de seguridad de la información

Los contenidos de la unidad 1 que tratan sobre conceptos básicos y fundamentales sobre la seguridad de la información se estudiarán entre la semana 1 y 2. Serán de utilidad para que usted tenga claro cuál es el proceso para asegurar los sistemas de información de una empresa, las actividades para crear un sistema de gestión de la seguridad, así como entender qué son los marcos de referencia o buenas prácticas para asegurar

la información. Le invito hacer una lectura comprensiva de los temas de esta unidad, así como el desarrollo de las actividades recomendadas para que pueda apoyarse y complementar el estudio de esta asignatura.

¡Iniciamos en el estudio de esta unidad!

1.1. ¿Qué es la seguridad de la información?

Antes de responder la pregunta ¿Qué es seguridad de la información? Es importante recordar la definición de dos términos por separado *información* y *seguridad*.

Para entender de mejor manera el concepto de información recordemos que un *dato* es un valor que se asigna a las cosas, por lo general conformado de letras o símbolos y pueden determinar un atributo o una característica de algo. Un dato solo o aislado no tiene sentido, pero si existen más datos y a estos se los organiza tendríamos como resultado *la información*. Es entonces que *la información* es un conjunto de datos organizados y con significado que tienen sentido para una persona o una organización y su objetivo es dar conocimiento de algo; y, *el conocimiento* es adquirir esta información para comprenderla, entenderla y razonarla dando como resultado el aprendizaje de una supuesta realidad.

Como ejemplo, pensemos en un solo *dato*, como un número formado por 10 dígitos, que por sí solo no nos da ningún mensaje o significado (ver figura 2). Sin embargo, si a este ejemplo le hacemos referencia el *número de cédula* o teléfono o quizá un *nombre y apellidos*, sabremos que puntualmente estamos hablando de *una persona* quizá que trabaja en cierta empresa asumiendo cierto rol (Esto último es el *conocimiento*).

Figura 2.

Ejemplo de datos, información y conocimiento



Departamento de Infraestructura

CI: 1104233729

Juan Pérez

57 años

Constructora Ortega S.A

Entonces, si la información genera conocimiento, esta se convierte en uno de los elementos o activos más importantes de una organización, el cual es utilizado en todos y cada uno de los procesos que utilizan sistemas de información para desarrollar sus productos o servicios. Esta información no solamente está almacenada en servidores, computadores o la nube, sino que puede estar escrita a mano en una agenda, informes, bitácoras o extraída en discos duros, etc.

La información es el resultado de datos manipulados y transformados por *sistemas de información* para luego ser usado por personas para diversas acciones, siendo la principal la toma de decisiones. Entonces ¿Qué es un sistema de información?

Desde un punto de vista general se puede definir a un *sistema de información* como colección de elementos que están orientados al *tratamiento de datos* para transformarlos en información y su uso posterior. Esta transformación tiene una base fundamental, se inicia de una necesidad de un usuario/cliente. El estudio de los sistemas de información surge como una subdisciplina de las ciencias de la computación, para racionalizar la administración de la tecnología dentro de las organizaciones. El concepto se ha ampliado hasta pasar a ser parte de estudios de otras ramas, es así como se pueden revisar investigaciones que están hablando de *sistemas de*

sistemas para referirse a los sistemas de información tecnológicos de las organizaciones

Pero las aplicaciones no están en la organización por sí solas, sino que están administradas por personas que siguen procesos definidos. Con la ayuda de equipos tecnológicos, todos estos elementos están relacionados directamente. Es así si la empresa desea contar con sistemas de información donde participan tecnología, personas y procesos. En la figura 3 podemos encontrar la relación de los componentes en el aspecto de tecnología como es el *hardware*, los sistemas operativos, el *middleware*, el *software de aplicación específico*, las personas que trabajan directamente con estos componentes y los procesos de la organización.

Figura 3.

Relación de los componentes de un sistema de información



Estos elementos deben interactuar a partir de los datos de entrada, procesarlos y obtener una información útil para un usuario. Podemos encontrar entonces sistemas de información de tipo gerencial, transaccional, ejecutivos, de toma de decisiones para la automatización de tareas, sistemas expertos, etc. etc.

Los sistemas de información por su propósito se pueden clasificar en tres grupos:

- *Transaccionales*, generalmente son los primeros que se han de implementar en una organización en un área determinada para solucionar un tema específico, asociado con la reducción de tiempos

de respuestas, optimización de tareas del personal, sus cálculos y trabajos son muy simples

- *Soporte a toma de decisiones*, son implementados en las organizaciones en el ámbito de la alta gerencia, consisten en el tratamiento de grandes volúmenes de datos. Entrega Información que permite apoyar a la toma decisiones en la organización.
- *Estratégicos*, se considera a aquellos sistemas que con el uso de la tecnología de la información permiten soportar o dar forma a la estrategia competitiva de la organización, o a su vez, apoyar el plan para incrementar o mantener la ventaja competitiva. No apoyan a la automatización de los procesos operativos de la organización ni proporcionan información para apoyar a la toma de decisiones.

Componentes de los sistemas de información

Desde el punto de vista de las TI, al sistema de información se lo puede definir como el sistema que permite obtener, almacenar, procesar y transmitir datos para satisfacer una necesidad de información. Definiremos también a los tres elementos que están presentes en los sistemas de información, que son necesarios para su funcionamiento y además, deben ser considerados como parte de los problemas de seguridad de la información que en lo posterior se pueden presentar. Estos componentes son:

- *Personas*: se debe tener claro que un sistema de información es desarrollado por personas y para personas. Desde el punto de vista del desarrollo, podemos encontrar quienes desempeñan diferentes roles dentro del proyecto, por ejemplo: analista, desarrollador. Como beneficiarios podemos encontrar personal interno de la organización y directivos de la misma, así como para usuarios finales.
- *Procesos*: una definición de la RAL Nos dice: *Conjunto de las fases sucesivas de un fenómeno natural o de una operación artificial*. Se define como una secuencia de procedimientos interdependientes y vinculados que, en cada etapa, consumen uno o más recursos para convertir insumos (datos, materiales, piezas, etc.) en productos. Estas salidas se sirven como insumos para la siguiente etapa hasta que se alcanza un objetivo o resultado.

- *Tecnología*, constituida por los siguientes elementos:
 - *Hardware*, según la definición de la Real Academia de la Lengua es *conjunto de los componentes que integran la parte material de una computadora*. En el caso de los sistemas de información no solo hace referencia a los componentes internos de la computadora, sino todos aquellos periféricos que son necesarios para su funcionamiento en un ambiente organizativo.
 - *Middleware*: es el medio que permite conectar dos aplicaciones y pasar datos entre ellas. Se lo conoce también como el *software* que permite un enlace entre aplicaciones *software* o *Software* según (Pressman, 2010). Son instrucciones que cuando se ejecutan proporcionan las características, función y desempeño.
 - El *software* de computadora como parte de un sistema de información se puede considerar a un producto que construyen los programadores
 - *Sistema operativo* sobre el cual se trabajará, pudiendo este variar para el mismo sistema, puesto que las capas de trabajo pueden ser diferentes (servidor de base de datos, aplicaciones, desarrollo etc.) o la infraestructura de telecomunicaciones que se utilice, así como los canales de comunicación entre los componentes.

Software aspecto central del sistema de información

La definición de *software* de computadora (Pressman, 2010) como el producto que construyen los programadores y al que se le da mantenimiento. Incluye programas que se ejecutan en una computadora de cualquier tamaño de arquitectura, así como también el contenido que se presenta a medida que se ejecutan los programas.

El *Software* de computadora se construye del mismo modo que cualquier producto exitoso, con la aplicación de un proceso ágil y adaptable para obtener un resultado de calidad que satisfaga las necesidades de las personas que usarán el producto. Desde el punto de vista del usuario es la información que se visualiza para hacer mejor un proceso que realiza diariamente, pero desde el punto de vista del ingeniero de *software* son programas de computadora complejos, realizados con alta calidad, bajo

estándares de programación, siguiendo una metodología de desarrollo adecuada y cumpliendo con las regulaciones del gobierno, las necesidades del cliente y factibilidades previamente definidas.



Hasta el momento no hemos dado respuesta a la pregunta con la que iniciamos el estudio de este contenido, pero es importante que recordemos lo que es un dato, información, conocimiento y sistemas de información para llegar a comprender a que nos referimos con *seguridad de la información*.

Si los sistemas de información son de vital importancia para una organización porque le apoyan a cumplir sus objetivos estratégicos. Es necesario proteger estos sistemas y sobre todo implantar seguridad a la información que estos manipulan o procesan. Entonces, entendemos como seguridad de la información a la *protección de la información contra la divulgación, transferencia, modificación o destrucción no autorizada ya sea accidental o intencional* (Webinar ISOTools, 2019). A pesar de ser un concepto simple abarca algunas definiciones las que vamos a contextualizar:

- a. ¿Qué se protege? La información, puesto que es el activo más importante de una organización.
- b. ¿De qué se la protege? Sobre todo de amenazas que son internas y externas y que están esperando una vulnerabilidad para poder materializarse. Por ejemplo, puede ser un puerto abierto en un servidor, un bucle mal cerrado en el código de un programa, el antivirus del computador no actualizado, etc.
 - a. ¿Qué es la divulgación? Que la información sea expuesta o dada a conocer a personas que por lo general no son dueños de la información y se convierte en una mala acción, en el momento que sabemos que dicha información es privada o tiene alguna restricción respecto a ser divulgada y hay malas intenciones de por medio.
 - b. ¿Qué es transferencia? Sucede cuando la información pasa de un emisor hasta un receptor por medio de un canal de información. Se ve afectada cuando en medio de esta comunicación, sea interceptada y manipulada o cambiada, o, en

el peor de los casos, destruida o eliminada. El principal pilar de seguridad afectado aquí es la integridad.

Pero ¿Cómo se protege la información?, la protección en sí misma no es una tarea o actividad fácil de implementar. Se puede denominar incluso como un proceso (un conjunto de actividades) donde se hace una implementación técnica de herramientas, tecnologías, normas, políticas, controles, buenas prácticas, etc. cuya finalidad es la protección de la información y de sus tres pilares fundamentales: confidencialidad, integridad y disponibilidad; y, también en algunos casos, según ciertos expertos, en temas de seguridad se toma en cuenta el *No repudio*. Este proceso de aseguramiento de información se ha convertido hoy en día en una herramienta de las organizaciones para mantenerse en el mercado, ser una empresa altamente competente y tener una rentabilidad alta, tomando en cuenta que la mayoría de las organizaciones utilizan tecnologías de la información (TI) para su funcionamiento y ofrecen servicios como comercio electrónico. Por ejemplo, Amazon.

La seguridad de la información está orientada a proteger toda clase de información o datos, sean o no utilizados por tecnologías de información, como, por ejemplo: actas e informes confidenciales, guardados generalmente en los archivos del departamento legal de una organización. Sea cual sea el tipo y clase de información de una organización siempre tiene un riesgo, que es el resultado de la combinación de dos factores, una amenaza y una vulnerabilidad.



En la tabla *Definiciones dentro de la de seguridad de la información*, del punto 1.3 de esta Unidad puede revisar la definición de amenaza y vulnerabilidad.

¿Por qué proteger?, porque constantemente los sistemas de información de las organizaciones están expuestos a amenazas y vulnerabilidades. En la tabla 1 se enlistan las amenazas de TI más comunes para estos sistemas de información.

Tabla 1.

Amenazas de TI más comunes

Amenazas de TI más comunes
Violaciones de datos
Protección insuficiente de los accesos
Interfaces y APIS inseguras
Vulnerabilidades del sistema
Secuestro de cuenta
Amenazas internas
Amenazas persistentes avanzadas
Pérdida de información
Due diligence insuficiente
Abuso y uso nefasto de los servicios en la nube
Negación del servicio
Vulneraciones de tecnología compartida

Nota. Adaptado de RITTAL, 2018. Principales riesgos y amenazas de seguridad IT.

Es importante también considerar como amenazas los siguientes factores que quizá están fuera del ámbito de TI, pero que afectan a algún elemento del sistema de información de la organización (tabla 2):

Tabla 2.

Otros factores de amenaza

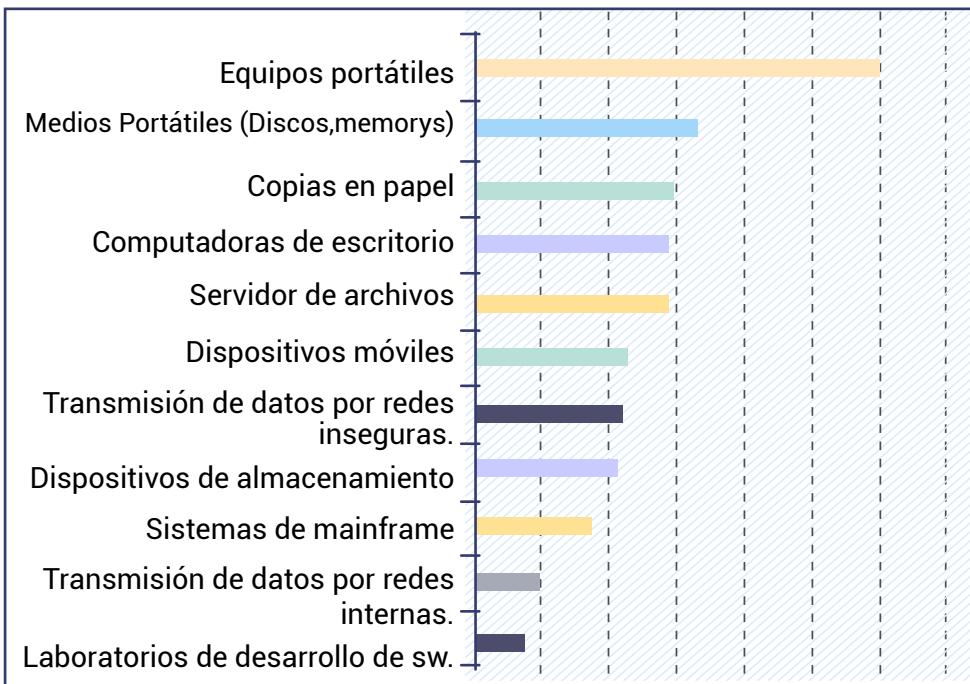
Otros factores de amenaza
Robo, fraude, hurto, espionaje, virus, etc
Incendios, inundaciones, Sismos, etc.
Negligencia del personal, no hay políticas ni normas de seguridad, no hay concienciación ni capacitación al personal de la organización.
Rotación de personal.
Pérdida de contraseñas
Mal almacenamiento físico de información
Mal manejo de computadores y software, etc.

Nota. Adaptado de RITTAL, 2018. Principales riesgos y amenazas de seguridad IT.

En la figura 4 en cambio, se describen los activos que son más vulnerables en una organización:

Figura 4.

Activos más vulnerables en una organización



Nota. Delgado, C. A. A., 2017. Fundamentos de seguridad informática.

Con base en esta figura se concluye que las laptops o portátiles hoy en día son blancos fáciles de ataques contra las organizaciones. Pues generalmente son manipulados por personas que son el eslabón más débil en la seguridad según (Aranda, 2016). Por lo tanto, es un activo cuya prioridad de proteger es alta porque también hay ciertas vulnerabilidades que por lo general pasan desapercibidas. Por ejemplo, antivirus no actualizado, un *malware* instalado, etc.

En el capítulo de gestión de riesgos se tendrá en cuenta mejor cómo se hace un adecuado análisis de activos para poder evaluar los riesgos y proponer contramedidas.

Podemos darnos cuenta de que las amenazas a las que está expuesto un sistema de información de una empresa son innumerables, al igual que las vulnerabilidades, es por esto por lo que el proceso de aseguramiento de la información tiene que ser visto como una actividad transversal en todas las áreas y recursos de una organización.

Tratar de asegurar los sistemas de información de una organización es un proceso amplio que empieza estableciendo o determinando objetivos de seguridad claros, que busquen mediante controles y lineamientos de seguridad siempre preservar los activos.

1.2. Objetivos de la seguridad de la información

Los objetivos de la seguridad de la información son lineamientos específicos que buscan mantener y garantizar *los tres pilares fundamentales de la seguridad de la información: la confidencialidad, integridad y disponibilidad* en cada uno de los activos de información de una organización. Estos objetivos son propuestos por expertos en el tema de seguridad de la información y la alta gerencia. A continuación se describen algunos ejemplos de objetivos de seguridad de la información que alguna organización podría querer lograr:

- Conservar la integridad de la información personal de los clientes.
- Proteger la confidencialidad de la información de los clientes y personal de la organización.
- Evaluar y tratar riesgos de TI para que permanezcan en niveles aceptables o tolerables para la organización, etc.

Sean cuales sean los objetivos de seguridad propuestos, siempre deben basarse en los pilares de seguridad de información antes mencionados y que a continuación se describen más detalladamente.

1.2.1. Pilares fundamentales de la seguridad de la información

En el siguiente recurso se describe que la base de la seguridad de la información son tres pilares fundamentales: la confidencialidad, la integridad y la disponibilidad. Por motivos de estudio también incluimos el No Repudio, pero se debe recordar que este no forma parte de estos pilares.

[Pilares de la Seguridad de la información](#)

1.3. Definiciones dentro de la seguridad de la información

En la tabla 3 se describen algunas definiciones básicas tanto para comprender el tema de seguridad de la información como para el estudio de las siguientes unidades de este texto guía.

Tabla 3.*Definiciones dentro de la de seguridad de la información*

Tema	Definición	Ejemplo
Amenaza	Se denomina a la posibilidad de que un evento o acción potencial se materialice por medio de una vulnerabilidad y cause daño, sobre todo a los sistemas de información de la organización durante cierto periodo de tiempo.	<p>En (Johanna Cárdenas Solano et al., 2014) se enlistan algunas amenazas:</p> <ul style="list-style-type: none"> ▪ Desastres naturales que afectan a la instalación física de la organización. ▪ Fallas en el suministro eléctrico, que afectan a la parte de <i>hardware</i> de la organización. ▪ Amenazas programadas tales como virus y bombas lógicas que afectan el <i>software</i>. ▪ Fallas de <i>hardware</i>. ▪ Fallas de <i>software</i>, corrompiendo los datos. ▪ Errores humanos que afectan a cualquier sistema de la organización.
Vulnerabilidad	Según NIST (National Institute of Standards and Technology) es la debilidad en un sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podrían ser explotados o desencadenados por una fuente de amenaza. Imaginemos que una vulnerabilidad es una puerta o ventana abierta de una casa por donde cualquier criminal pueda ingresar.	Según (Guamán & Jaramillo, 2018) algunas vulnerabilidades denominadas lógicas se refieren a las fallas en aplicaciones dadas por la falta de seguridad o por errores propios y por los cuales personas no autorizadas pueden ingresar sobre todo tener acceso a los activos de la organización.

Tema	Definición	Ejemplo
Riesgo	Riesgo es un posible evento que podría causar daños o pérdidas o afectar la capacidad para lograr los objetivos. Un riesgo se mide por la probabilidad de una amenaza, la vulnerabilidad del activo a esa amenaza y el impacto que tendría si ocurriera. También se puede definir como la incertidumbre del resultado y se puede utilizar en el contexto de la medición de la probabilidad de resultados positivos y negativos.	Indisponibilidad de los servicios de red. Indisponibilidad de servicios y servidores. Extracción, modificación y destrucción de información confidencial. Uso inadecuado de infraestructura de TI. Inadecuados controles de acceso lógico.
Ataque	Un ataque es una amenaza a la seguridad de la información que implica un intento de obtener, alterar, destruir, eliminar, implantar o revelar información sin acceso o permiso autorizado. Un ataque puede ser tanto a personas como a organizaciones.	Hay muchos tipos diferentes de ataques, incluidos entre otros: pasivos, activos, dirigidos, botnet, phishing, spam, internos y externos.

Finalmente, hemos culminado la semana 1 de estudio. Usted debería estar en la capacidad de responder las siguientes interrogantes ¿Qué entiende por seguridad de la información? ¿Cuáles son los principales objetivos que se logran con la seguridad de la información? ¿Cuáles son los principales pilares de la seguridad de la información? ¿Qué es disponibilidad, integridad y confidencialidad? ¿Qué es un riesgo? ¿A qué nos referimos con amenazas? Es importante que considere revisar conceptos básicos estudiados en ciclos anteriores con la finalidad de que en los siguientes temas sea más sencilla la comprensión de estas.





Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

Lecturas en bibliografía básica, complementaria y recursos educativos abiertos

- Revise la bibliografía complementaria para reforzar sus conocimientos respecto a los temas propuestos en la semana 1 de estudio.
- Cryptography and Information Security (Capítulo 1: Introduction 1.1 Security, 1.2 Elements of Information Security, 1.3 Security Policy)
- Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades (Capítulo 2: Fundamentos de la Ciberseguridad, subtemas del 2.1. al 2.3.)

▪ Actividad 1:

Descargue el siguiente análisis [CIBERSEGURIDAD EN ECUADOR](#) y desarrolle las siguientes preguntas: ¿Cuáles son las tendencias en Gestión de Ciber Riesgos y Seguridad de la Información en el Ecuador? ¿Qué estrategias han realizado las organizaciones para contener estos Ciber Riesgos? ¿Cuáles son los controles o buenas prácticas según su criterio que debería incluir también las organizaciones?

Nota. Conteste las actividades en un cuaderno de apuntes o en un documento de Word.

Resultado de aprendizaje 2 y 3

- Describe los elementos que contribuyen al coste de la gestión de seguridad de una organización, políticas de seguridad y procesos operativos relacionando los riesgos y pérdidas asociadas con la seguridad de la información.
- Describe la importancia de utilizar estándares actualmente usados en aseguramiento de la información y sus áreas de relevancia.

Una vez que se han estudiado conceptos básicos es importante conocer que la implementación de la seguridad de la información no es un simple proceso. Su enfoque dentro de una organización es sumamente holístico, es decir, buscar el aseguramiento de los activos de la información que esta considere los más importantes y que pueden ser de cualquier tipo, sea *software*, *hardware*, infraestructura, personas y aquellos activos que forman parte del sistema de información de la organización. Con la finalidad de que este proceso se convierta en un proceso formal es importante que analicemos algunos estándares utilizados para la seguridad de la información.

Contenidos, recursos y actividades de aprendizaje



Semana 2

1.4. Estándares usados para la seguridad de la información

Lo primero que tiene que hacer una organización es tener claro que la seguridad de la información será un proceso donde se desarrollarán un conjunto de documentos con políticas estándares, directrices o controles que apoyen esta importante tarea. Este proceso debe llegar a cumplir las metas, los objetivos y los requisitos del programa de seguridad de la organización y sobre todo establecer los controles mínimos para el funcionamiento adecuado de los sistemas y aplicaciones de información.

Para proporcionar cierta estructura a este proceso es importante que la organización o quién esté a cargo de la seguridad de la información adopte un marco de referencia, una guía, un estándar o un *framework* para guiar el desarrollo y garantizar la cobertura adecuada en todos los niveles que la seguridad se requiera.

Un marco de referencia: *framework*, guía o norma es una estructura que nos indica qué/cómo una tarea o actividad determinada debe desarrollarse y en su mayoría son documentos creados por organizaciones, algunas sin fines de lucro y que han sido aplicados en organizaciones cuyos resultados de aplicación han sido de alguna manera beneficiosos. Como se ha mencionado anteriormente, el proceso de la seguridad de la información debe estar basado en un estándar, marco de referencia o norma para que su gestión sea mucho más sencilla. Al aplicar un estándar se garantiza que en el sistema de información se están asegurando todos los elementos esenciales y que se relacionan y se apoyan entre sí.

Landoll (2017) menciona algunos beneficios que se tienen al establecer la seguridad de la información, basados en políticas, ya que son de mucha utilidad y la base fundamental para empezar con este proceso será un soporte para la Auditoría de Sistemas de Información que en las organizaciones es una tarea que se la realiza de manera anual.

A continuación, se describen algunos estándares que usted podría utilizar como guía para el proceso de aseguramiento de la información.

1.4.1. FISMA Framework

FISMA define una guía para la gestión de la seguridad de la información para todos los sistemas de información utilizados u operados por una agencia del gobierno federal de los Estados Unidos en las ramas ejecutiva o legislativa, o por un contratista u otra organización en nombre de una agencia federal en esas ramas. Este marco se define además por las normas y directrices desarrolladas por el NIST (National Institute of Standards and Technology).

Es importante conocer cuál fue el objetivo por el que fue creado este estándar y si puede servir de apoyo a que cualquier organización logre un nivel de seguridad estable. El documento central de este estándar es la Publicación Especial (SP) 800-53: Controles de seguridad y privacidad para sistemas y organizaciones de información. Este documento proporciona una

guía útil para la organización y construcción de políticas de seguridad de la información.

En la tabla 4 se observan las familias de controles que maneja este estándar.

Tabla 4.

Familia de controles del estándar FISMA

ID	CONTROL FAMILY
AC	Control de Acceso
AT	Sensibilización y formación
AU	Auditoría y rendición de cuentas
CA	Evaluación y autorización de seguridad
CM	Gestión de configuración
CP	Planificación de contingencias
IA	Identificación y autentificación
IR	Respuesta a Incidentes
MA	Mantenimiento
MP	Protección de medios
PE	Protección física y de medioambiente
PL	Planificación
PS	Personal de seguridad
RA	Administración de riesgos
SA	Adquisición de sistemas y servicios
SC	Protección del sistema y las comunicaciones
SI	Integridad de sistemas y servicios
PM	Gestión de Programas

Nota. Adaptado de Landoll, D. J., 2017.

Este estándar no solo proporciona una organización de alto nivel de controles de seguridad de la información, sino también requisitos detallados sobre controles, procesos, tecnología y técnicas. Estos requisitos individuales proporcionan a la organización requisitos específicos para completar cada una de las políticas de seguridad de la información que vayan a ser creadas basadas en FISMA. Al igual que algunos otros estándares estas políticas pueden modificarse o reorganizarse según sea necesario. La reorganización de algunos de los elementos de política puede ser necesaria para agrupar elementos de política similares y crear claridad y coherencia dentro de las políticas y el conjunto de políticas. En la figura 5 se puede ver un ejemplo claro de cómo pueden quedar reorganizados los controles de seguridad de FISMA, agrupados en 4 políticas de seguridad de la información con un total de 17 políticas.

Figura 5.

Reorganización de controles de seguridad de la información en cuatro políticas



Nota. Adaptado de Landoll, D. J., 2017.

Uno de los beneficios de utilizar este estándar es que está basado en el documento NIST SP 800-53 donde hay una guía complementaria para explicar y proporcionar una relación para casi todos los controles. Además, el NIST ha elaborado un extenso catálogo de publicaciones especiales (serie 800) que brindan orientación de apoyo sobre muchos temas de seguridad y privacidad de la información.

1.4.2. Estándar ISO 27001:2013

Es un estándar de seguridad de la información creado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) y aunque se la conoce como la ISO 27001, pero su nombre es *Information Technology—Security Techniques—Information Security Management Systems— Requirements*. El estándar es una especificación para establecer un *Sistema de Gestión de Seguridad de la Información (SGSI)*.

Un SGSI es un conjunto de políticas, procedimientos y procesos organizados que establecen los requerimientos y el proceso para implementar un conjunto de controles físicos, administrativos y técnicos para proteger los activos de información de la organización. Este SGSI debe estar alineado a la estrategia del negocio (misión, visión, valores y objetivos de la organización). También busca ser el medio más eficaz para minimizar los riesgos, ya que establece que se deben identificar activos y valorar riesgos a los que estos activos están expuestos, tomando en cuenta siempre el impacto que se dará a la organización si estos riesgos se materializan. Este estándar está formado por 7 cláusulas y una referencia a 114 controles dentro de 14 grupos.

Para entender este estándar se debe considerar que está basado en el ciclo de Deming, buscando siempre la mejora continua. El ciclo de Deming tiene 4 bases: planificar, hacer, comprobar y actuar, o, con sus siglas en inglés PDCA. Se define brevemente a qué actividades se refiere o se tienen que realizar en cada etapa:

- *Planificar:*
 - Se hace un estudio de la organización respecto a su situación en torno a medidas de seguridad, para estimar qué medidas plantear o para evaluar las que ya se han planteado con anterioridad. También se puede denominar a esta parte como establecer los requisitos de seguridad de la organización.
 - Para evaluar estas medidas se debe hacer una correcta gestión de riesgos de los principales activos de información de la organización para saber cuáles son las amenazas más potenciales y las vulnerabilidades por las que estas pueden materializarse. Esta actividad está orientada a una ardua planificación de riesgos en los activos.

- *Hacer*
 - Se realizan todas las actividades planificadas en el plan de gestión de riesgos y se incluye el tratamiento de estos con la implementación de controles.
 - Cada control de seguridad que se implementa debe estar basado en una política de seguridad y todo debe estar documentado y registrado, todo proceso, quién lo ejecuta, cómo se implementó o se implementa.
 - Se comunica finalmente a todas las partes interesadas y se concientiza a todo el personal, sobre todo de las políticas que se deben cumplir.
- *Comprobar*
 - Los controles o medidas implementadas deben ser verificadas en tema de su cumplimiento, con base en registros e indicadores.
 - Verificar que el SGSI implementado funciona correctamente.
- *Actuar*
 - Implementar contramedidas si son necesarias.
 - Se actualiza controles dependiendo de si se utiliza estándares o buenas prácticas.
 - Actividades de mejora y corrección del SGSI.

En la tabla 5 se muestra a la izquierda la estructura del documento de la ISO 27001 y a la derecha se muestra un resumen de los controles o requisitos de seguridad sugeridos por esta norma.

La mayoría de las organizaciones cuando quiere asegurar sus sistemas de información e implantar un SGSI, combina por lo general la ISO 27001 y los controles del Anexo A, con los controles que se encuentran establecidos en la ISO 27002, esto se ha convertido en una buena práctica.

Tabla 5.

Estructura del documento del estándar ISO 27001 y resumen de los controles del Anexo A

SGSI ESTANDAR	ISO/IEC 27001:2013	Controles	ISO/IEC 27001:2013 – Anexo A
	Introducción	A5	Políticas de seguridad
1	Alcance	A6	Organización de la Seguridad de la información
2	Referencias Normativas	A7	Seguridad Recursos Humanos
3	Términos y Definiciones	A8	Gestión de activos
4	Contexto de la organización	A9	Control de acceso
5	Liderazgo	A10	Criptografía
6	Planificación	A11	Seguridad física y ambiental
7	Apoyo	A12	Seguridad de operaciones
8	Operaciones	A13	Seguridad de las comunicaciones
9	Evaluación del desempeño	A14	Adquisición, desarrollo y mantenimiento de los SI.
10	Mejora	A15	Relaciones con suministradores
		A16	Gestión de incidentes en la Seguridad de la información.
		A17	Aspectos de seguridad de la información en la gestión de continuidad de negocio.
		A18	Cumplimiento

Nota. Tomado de Estructura de la norma ISO 27001. (2013). [Gráfico]. <https://www.iso27000.es/assets/images/soa1-826x378.png>

Los beneficios de implementar un SGSI son algunos. Por ejemplo:

- Una organización al implementar un SGSI será sin ninguna duda un arduo competidor en el mercado.
- Reducirá los riesgos considerablemente en torno a los activos de información más importantes para la organización.
- Optimización de recursos y un aumento considerable de la eficiencia y eficacia de procedimientos y operaciones.
- Se establece un nivel de madurez en la gestión de la seguridad de la información.
- Se evalúa el cumplimiento legal con terceros.
- Por lo antes descrito, la organización aumenta el valor y ganancia en el mercado.

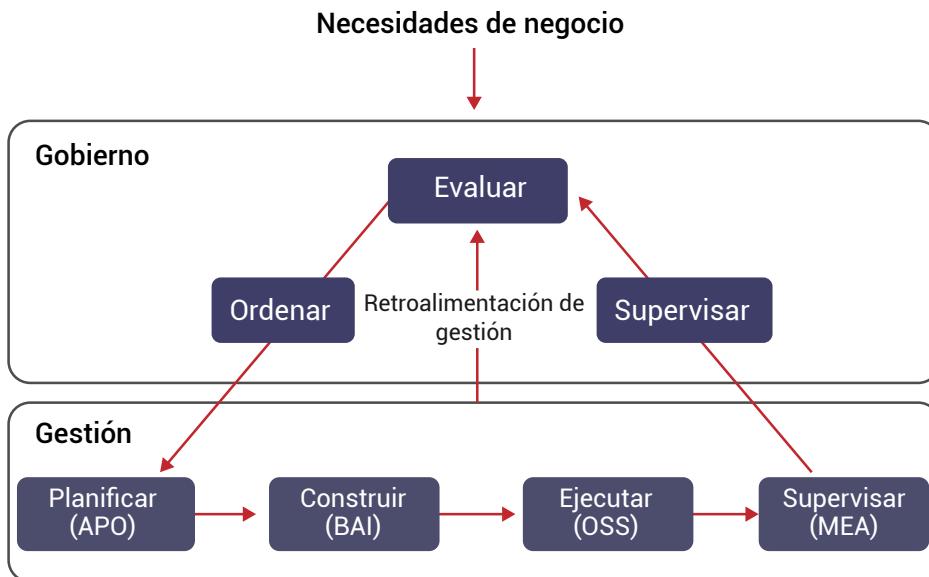
- Por los controles implementados se crea un proceso de continuidad de negocio en mejores condiciones.
- La ISO proporciona algunas pautas de implementación, gran cantidad de capacitación, orientación y asistencia, ya que es un estándar mundialmente conocido y está disponible a través de grupos comerciales.
- Se puede unir o relacionar con otras normas que están disponibles en ISO/IEC, NIST, US-CERT y otros grupos.

1.4.3. Marco de referencia COBIT

COBIT es un marco de control de gestión y gobierno de TI creado por la Asociación de Control y Auditoría de Sistemas de Información (ISACA). Se utiliza principalmente para establecer y administrar un conjunto de controles de gobierno y de TI. La estructura básica de este marco de referencia también proporciona la base para un SGSI.

Los controles de gestión y gobierno de TI de COBIT están organizados en cuatro dominios: Alinear, planificar y organizar, Construir, adquirir e implementar, entregar, dar servicio, soporte y supervisar, evaluar y Valorar. Cada dominio tiene procesos, son un total de 11 en los 4 dominios y 5 procesos más de gobierno de TI empresarial. En la figura 6 se puede observar las áreas de Gobierno y Gestión que cubre COBIT 5.

Figura 6.
Marco COBIT 5



Nota. ISACA. (2012). COBIT 5.

El modelo de referencia de procesos COBIT 5, se lo puede distinguir en el documento Procesos Catalizadores COBIT 5. Hay que tomar en cuenta que los primeros procesos que busca implementar este marco de referencia son los procesos de Evaluar, Orientar y Supervisar, que tienen que ver primero con el Gobierno de TI del negocio.

Procesos Catalizadores COBIT 5

Landoll, 2017 explica que dentro de cada dominio hay un conjunto de procesos diseñados para cumplir con los objetivos de la organización. Cada proceso se numera secuencialmente dentro del dominio (por ejemplo, P01, P02). Cada uno de estos procesos puede tener uno o más objetivos de control asociados (por ejemplo, P01.1, P01.2). Estos objetivos de control, a su vez, se cumplen mediante un conjunto de controles. Por ejemplo, el dominio de *Planificar y Organizar* (PO) tiene el proceso asociado P02: *Definir la Arquitectura de la Información*. El proceso de P02 tiene varios objetivos de control asociados, incluido P02.e: *Esquema de clasificación de datos*. El objetivo de control de P02.3 se cumple a través de seis controles que definen la creación de un esquema de clasificación de datos, definición de niveles de clasificación, identificación de dueños de negocios, clasificación

de datos dentro del esquema, educación sobre responsabilidad y etiquetado de datos y medios.

COBIT no es un marco de referencia orientado específicamente para establecer políticas de seguridad de información como otros marcos o estándares porque se centra más en establecer controles para las TI. Sin embargo, tiene objetivos de control que pueden ayudar a establecer una base específica para crear un SGSI.

Las ventajas más conocidas de este marco de trabajo son:

- Es un marco utilizado por algunas organizaciones en el mercado, para establecer procesos de control.
- Con este marco se está en la capacidad de definir controles con respecto a gestión y gobierno de TI por lo que lo convierte en un marco holístico de negocio.
- Es de fácil comprensión para el Gobierno de negocio.
- Optimización de recursos y costos de TI.
- Existe una alta documentación y guías para su implementación.
- Puede interrelacionarse con la ISO 27001, ITIL y otros marcos de referencia.

1.5. Sistemas de gestión de seguridad de la información SGSI

Según la ISO 27001:2013 un SGSI está conformado por una serie de procesos para implementar, mantener y mejorar de forma continua la seguridad de la información con base en los riesgos que afectan a los activos de información de una organización.

Le invito a profundizar sus conocimientos acerca de este importante tema:

En el punto 1.4.2 del texto guía se estudió brevemente la ISO 27001 que es un estándar para implantar un SGSI, dándonos una idea general a lo que nos referimos con Sistemas de Gestión de Seguridad de la Información. Para (Guamán & Jaramillo, 2018) el principal objetivo de un SGSI es garantizar que los riesgos de los activos de información de una organización sean

conocidos, asumidos, gestionados y minimizados por la organización, de una manera sistemática, estructurada, eficiente y adaptada, sobre todo documentada y que se convierta en un proceso sencillo y sea un apoyo fundamental en el aseguramiento de los activos de la empresa.

Se ha revisado también conceptos como la seguridad de la información y de sus pilares fundamentales, que es siempre preservar la confidencialidad, integridad y disponibilidad de la información y de todos los sistemas de información dentro de una organización.

Un SGSI puede ser estructurado con más estándares o marcos de referencia como apoyo. Por ejemplo, la ISO 27002 por lo general va en conjunto con la aplicación del Anexo A de la ISO 27001. Podemos utilizar ITIL, ISM3, ISO 31000 para ejecutar la fase de gestión o evaluación de riesgos y para la parte de dar respuesta al riesgo, estableciendo controles. Se puede utilizar: ISO 27001 Anexo A y 27002, también COBIT 5.

Antes de verificar cuáles serían las fases para implementar un SGSI según la ISO 27001, vamos a indicar algunos puntos relevantes de por qué es bueno implementar un SGSI en una organización.

- Buscar siempre la mejora continua de la organización, es decir, implementar una cultura de la seguridad en la organización donde será aplicada y cuyos controles de seguridad de información serán aplicados de manera progresiva.
- Un SGSI se ajusta a las necesidades de la organización en la que será implementado porque establece que se debe hacer un proceso de análisis de riesgos de los activos de información y procesos propios de la organización.
- Determinar un tratamiento adecuado para estos riesgos se enfoca principalmente a buscar de una manera directa la seguridad de la información de la empresa.
- Si se implementa un SGSI en base a la 27001 se tendrá una apertura para la integración con otros sistemas de gestión, por ejemplo, la ISO 9001 o la ISO 14001.

1.5.1. Implementación de un SGSI según la ISO 27001

Para entender la implementación de un SGSI en una organización, tomaremos como referencia el ciclo de Deming (Planificar, Hacer, Comprobar y Actuar). Lo importante es también tener claro que la implementación de un SGSI es un proceso que se lo debe considerar como cuando se implementa cualquier clase de proyecto en la organización, es decir, proveer recursos (personas, software, hardware infraestructura) y también recursos financieros, sobre todo si se tiene en mira el buscar la certificación o solo el objetivo de asegurar el/los sistemas de información de la organización.

Una vez comprendido el documento de la norma se puede definir las actividades de implementación de acuerdo con las fases del ciclo de mejora continua. Algunas de estas actividades están descritas en la tabla 6.

Tabla 6.

Actividades por cada fase del ciclo de Deming de la ISO 27001

FASE DE CICLO DE DEMING	ACTIVIDADES
Planificar	<ul style="list-style-type: none">▪ Definir del alcance SGSI▪ Definir la política de seguridad, que establecerá la base del SGSI▪ Definir una metodología de evaluación y tratamiento de riesgos.▪ Identificar activos y riesgos que se encuentren dentro del alcance.▪ Determinar el valor del riesgo de los activos.▪ Determinar el tipo de tratamiento de riesgo,▪ Documentación aprobada por la alta dirección▪ Definir el proceso de implementación de los controles identificados.
Hacer	<ul style="list-style-type: none">▪ Definir e implantar el plan de tratamiento de riesgos.▪ Determinar las variables o indicadores que ayuden a determinar si los controles implementados están funcionando.▪ Concientizar y formar al personal de la organización.▪ Administrar las operaciones y procesos con los que funcionará el SGSI▪ Definir e implantar los procedimientos que ayuden a resolver incidentes de seguridad.

FASE DE CICLO DE DEMING	ACTIVIDADES
Comprobar	<ul style="list-style-type: none"> ▪ Revisión de procedimientos establecidos para detectar errores. ▪ Revisión de efectividad de controles implantados. ▪ Auditoría y revisión del SGSI ▪ Gestión de cambios del SGSI o de la organización. ▪ Revisar el alcance del SGSI ▪ Documentar eventos o acciones que impacten la efectividad del SGSI
Actuar	<ul style="list-style-type: none"> ▪ Implementar planes de mejora. ▪ Comunicar planes de mejora de acciones correctivas. ▪ Asegurar la consecución de los objetivos del SGSI

Nota. Elaboración propia.

Para implementar un SGSI en una organización hay algunas fases a tomar en cuenta que se describen a continuación.

1.5.2. Fases de Implementación de un SGSI según la ISO 27001

Las fases que la mayoría de las organizaciones debe seguir para implantar el SGSI, se enlistan enseguida:

- **Fase 1:** Se hace la planificación del proyecto para implantar el SGSI, se realiza el análisis GAP (Comparación del desempeño real con el deseado) y se cumple con la cláusula 4 de la norma, que es entender el contexto de su organización para identificar los activos de información importantes.
- **Fase 2:** Gestión de Riesgos y se planifica la acción que se llevará a cabo para tratarlo.
- **Fase 3:** Documentar el proceso de SGSI y cada una de las cláusulas de la norma, se define el proceso de comunicación con un enfoque de concientización, se evalúa las operaciones y se constituye los indicadores de gestión, a la par de todas estas actividades se pone ya en marcha el SGSI.
- **Fase 4:** Se pone en marcha el SGSI en su totalidad y se empieza a documentar y estudiar indicadores de funcionamiento, lo que nos sirve para hacer una Auditoría Interna de lo que se ha implantado, para

verificar que el proceso del SGSI haga lo que debe hacer y que los controles funcionen correctamente, en caso de haber anomalías se pasa a la fase 5.

- *Fase 5:* Se realizan las acciones correctivas, con esto se cumple con el propósito de mejora del SGSI. Se comunica los cambios implantados.

1.6. Auditoría de un Sistema de gestión de seguridad de la información SGSI

Las auditorías de los SGSI se las realiza para determinar la eficiencia y eficacia del SGSI como tal.

En esta auditoría se dimensiona el alcance dependiendo del tamaño y naturaleza de la organización que tiene el SGSI y también de cuán complejo es el SGSI que se va a evaluar. (Merino & Cañizares, 2014) mencionan que no es lo mismo auditar un SGSI recién implantado cuyo nivel de madurez será bajo, que auditar un SGSI que ya lleva varios años establecido dentro de un proceso de mejora continua con un elevado nivel de madurez.

Establecer una auditoría es como implantar un proyecto, se requieren todos los recursos necesarios para llevarla a cabo, como tener en claro algunas actividades a cumplir dentro de estas.

1.7. Fases de auditoría de un SGSI

Las fases que se implementan para la auditoría de un SGSI son:

- *Fase 1:* se define la auditoría del SGSI como un proyecto y se provee de recursos necesarios para poder realizarla, se define también los objetivos de la auditoría, teniendo en claro qué se quiere lograr con esta evaluación. El tiempo que llevará a cabo lograr estos objetivos también se los determina en esta fase, así como los siguientes elementos: procedimientos, criterios, métodos de la auditoría y se determina el equipo auditor.
- *Fase 2:* el documento de salida de esta fase es el plan de auditoría del que está encargado el auditor en jefe, aquí se describen todas las actividades a tomar en cuenta en la auditoría y cuál será la

repercusión en los procesos de la Organización. Las actividades serán más detalladas como: quién las realizará y en qué tiempo se llevarán a cabo, (Merino & Cañizares, 2014) también mencionan que aquí se determinan las técnicas de muestreo que se implementarán y sobre todo los riesgos derivados de la realización de la auditoría. En el documento que es el plan inicial deben constar según (Merino & Cañizares, 2014):

- Objetivos de la auditoría.
 - El alcance de la auditoría, incluyendo los procesos y las áreas que serán auditadas.
 - Los criterios de auditoría y cualquier documento de referencia pueden ser de informes de auditorías anteriores.
 - Las técnicas de muestreo a utilizar y la metodología con la que se hará esta auditoría, sobre todo especificar el proceso de obtención de muestras.
 - Las responsabilidades de cada uno de los que conforman el equipo auditor, así como otras personas que participaran dentro de la auditoría, las que se deben entrevistar o que participan como guías u observadores.
- Fase 3: ejecución de la auditoría. Aquí se comprueba que esté implementado el SGSI y que está en funcionamiento dentro del proceso de mejora continua, se analiza sobremanera la documentación registrada, manuales y políticas de seguridad establecidas. Se hace los acercamientos necesarios para que el equipo auditor conozca a fondo la razón de ser de la organización y si el SGSI está ayudando a cumplir sus objetivos estratégicos. También se verifican si se aplicaron las acciones correctivas y preventivas, según (Merino & Cañizares, 2014) mencionan que el SGSI debe cumplir una serie de requisitos mínimos, como:
- Requerimientos generales.
 - Establecimiento y mantenimiento del SGSI:
 - **Establecimiento del SGSI.**
 - **Implementación y operación del SGSI.**
 - **Monitorización y revisión del SGSI.**

- **Mantenimiento y mejora del SGSI.**
- **Requisitos documentales: procedimientos generales, control de documentación, control de objetivos...).**
- Auditorías internas.
- Revisión por la dirección:
 - **Aspectos generales.**
 - **Entradas de la revisión.**
 - **Salidas de la revisión.**
- Mejora del SGSI:
 - **Establecimiento de la mejora continua.**
 - **Acciones correctivas.**
 - **Acciones preventivas.**

Dado que esta fase es la más larga del proceso de auditoría, aquí también se analizan los procesos implementados para la gestión de riesgos, pero también qué tanto se cumplen los controles implementados, las políticas establecidas y los procesos definidos, se recopila las evidencias necesarias sobre todo para los aspectos legales, reglamentarios y contractuales. El Anexo A de la ISO 27001 y la 27002 es una herramienta para ir verificando junto con las variables e indicadores preestablecidos el cumplimiento e ir estableciendo contramedidas, en caso de que no se cumplen estos controles.

- **Fase 4:** ya finalizadas las actividades y tareas en la fase de ejecución que estuvieron planificadas y preestablecidas en el plan de auditoría, se finaliza la auditoría con un informe que se presenta al ejecutivo de la organización y una vez aprobado se hace la debida comunicación de este. Es importante mencionar que se puede auditar el SGSI con mira a la obtención de la certificación. En ese caso, el equipo auditor puede ser externo y esta documentación debe ser registrada para obtener esta certificación.

Hemos finalizado el estudio del contenido planificado para la semana 2. Es necesario que tenga muy claro cuáles son los estándares o normas más utilizados para la seguridad de la información, la implantación y auditoría de un SGSI. Recuerde apoyarse en bibliografía complementaria disponible digitalmente para que complete su estudio y se recomienda desarrollar las actividades de aprendizaje recomendadas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

Lecturas en bibliografía básica, complementaria y recursos educativos abiertos

- Libro de Implantación de un SGSI según la ISO 27001 (Capítulo 4: Actividades de implantación de un SGSI).
- Libro de Auditoría de un SGSI (Capítulo 3: Auditoría de Sistemas de Gestión. Capítulo 4: Proyecto de Auditoría de un SGSI).
- Normaiso27001 (Guía de implementación ISO 27001 paso a paso).

▪ **Actividad 1:**

Con base en la revisión de la bibliografía y recursos educativos abiertos sugeridos para su estudio y los que usted puede adicionar, por favor mencione las similitudes y diferencias entre los estándares utilizados para el aseguramiento de información.

- **Actividad 2:**

Basándonos en las lecturas realizadas respecto a la implementación de un SGSI, realice un Diagrama de Proceso que indique las actividades y el proceso en sí de implantación de la ISO 27001 en una organización.

Nota. Conteste las actividades en un cuaderno de apuntes o en un documento de Word.

Una vez que ha estudiado los conceptos relacionados con la Unidad 1, le invito a desarrollar la Autoevaluación con el fin de evaluar los conocimientos adquiridos hasta el momento.

¡Éxitos en la autoevaluación!



Autoevaluación 1



Una vez que ha estudiado los conceptos relacionados a la unidad 1, le invito a desarrollar la autoevaluación 1 con el fin de evaluar los conocimientos adquiridos hasta el momento.

¡Éxitos en la autoevaluación!

1. La información es:

- a. Un conjunto de datos ordenados y con sentido.
- b. Un conjunto de datos desordenados y sin sentido.
- c. Un conjunto de datos ordenados y sin sentido.

2. ¿Cuál de los siguientes no se considera un elemento de un sistema de información?

- a. Personas.
- b. Información.
- c. Controles.

3. La característica de la información exacta y completa significa que:

- a. Aumenta el conocimiento y reduce la incertidumbre.
- b. Precisa es lo que se necesita y lo que se busca.
- c. Tiempo en el que se necesita.

4. La divulgación es cuando:

- a. La información es expuesta a personas que no son dueños de la misma.
- b. Pasa de un emisor a un receptor.
- c. Se valora como el activo más importante.

5. Escoja al menos una amenaza de TI:

- a. Incendios.
- b. Negación de servicios.
- c. Inundaciones.

6. La confidencialidad:

- a. Cuida que los datos en su transmisión no sean alterados.
- b. Funciona sin interrupciones del sistema.
- c. Especifica que el personal tiene acceso a la información.

7. ¿Qué es una amenaza?

- a. Es una debilidad en el diseño de un sistema informático.
- b. Es cuando un evento se materializa por una vulnerabilidad.
- c. Es la posibilidad de que suceda un incidente por una vulnerabilidad.

8. ¿Qué es un ataque?

- a. Es una debilidad en el diseño de un sistema informático.
- b. Es cuando un evento se materializa por una vulnerabilidad.
- c. Es una amenaza a la seguridad de la información.

9. ¿Cuál de las siguientes es una norma que ayuda a establecer un SGSI?

- a. COBIT.
- b. ITIL.
- c. ISO 27001.

10. ¿Cuál de las siguientes buenas prácticas se basa en el ciclo de Deming?

- a. COBIT.
- b. ITIL.
- c. ISO 27001.

Puede verificar las respuestas de esta autoevaluación al final del Texto Guía.

[Ir al solucionario](#)

Si su puntaje no es bueno es importante que vuelva a revisar los contenidos de la unidad y los recursos de aprendizaje, no olvide que puede interactuar con su tutor por cualquier medio de comunicación que brinda la UTPL para que aclare sus inquietudes.

Resultado de aprendizaje 4

- Identificar riesgos asociados con desastres o interrupciones y especifica las principales estrategias de mitigación ante una situación para recuperación ante desastres, con base en un informe de Análisis de Impacto de Negocios (BIA).

Para hacer un adecuado proceso de seguridad de un sistema de información de una organización es importante identificar riesgos asociados a los activos de TI más importantes que esta posee para tomar decisiones y desarrollar propuestas que ayuden a prevenir, mitigar o reducir los riesgos existentes, así como desarrollar un tipo de contingencia o respuesta si el riesgo se materializa. Es por ello por lo que en esta unidad vamos a estudiar el proceso de gestión de riesgos, las buenas prácticas en las que algunas organizaciones se apoyan para establecer este proceso.

¡Éxitos en el estudio de esta unidad!

Contenidos, recursos y actividades de aprendizaje



Semana 3

Unidad 2. Gestión de riesgos

2.1. ¿Qué es la gestión de riesgos?

La gestión de riesgos son todas las medidas implantadas para controlar los riesgos en una organización y que tiene que ver con: analizarlos, tratarlos, aceptarlos y comunicarlos, no solo se comunica los riesgos, sino el proceso de control de estos y a todas las partes interesadas. La gestión de riesgos es eficaz cuando en primera instancia se identifica los riesgos y amenazas potenciales que sean muy probables que se materialicen por la existencia de vulnerabilidades en los activos principales de la organización y termina cuando se ha hecho un adecuado tratamiento de estos riesgos.

Establecer la gestión de riesgos en una organización es como implementar un proceso, el mismo que tiene fases, actividades y tareas orientadas a

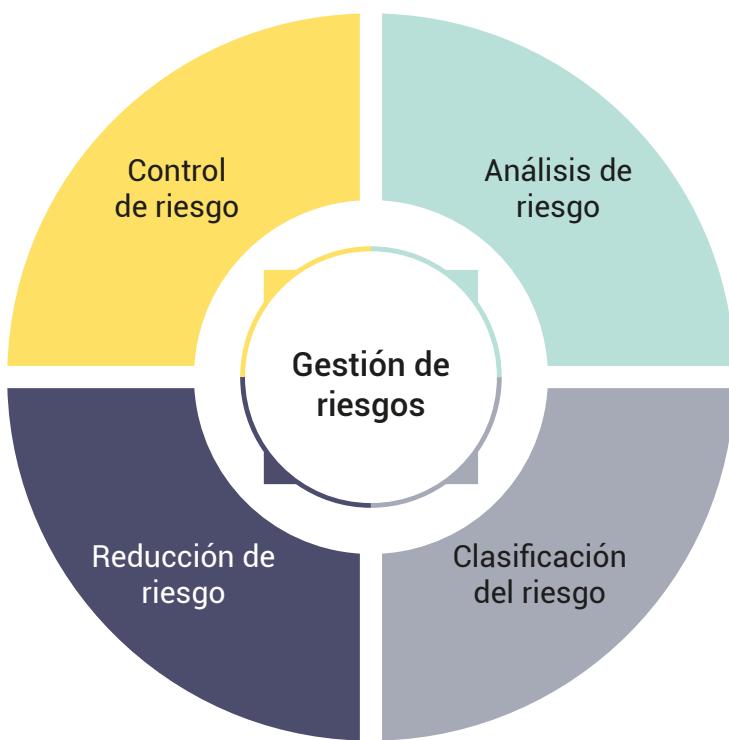
determinar y tratar los riesgos más potenciales que posiblemente afectaría a sus activos. Revisemos entonces el proceso de gestión de riesgos.

2.1.1. El Proceso de gestión de riesgos

Toda organización se encuentra expuesta a muchas vulnerabilidades y amenazas suscitadas por el uso de las TIC, por lo que es importante proteger los activos de información más importantes y es aquí cuando la gestión de riesgos es un proceso clave para garantizar y proteger estos activos como son según (Montaña, 2016): las personas, los datos sensibles, las bases de datos, la infraestructura de red y las aplicaciones.

En la figura 7 se describe el proceso general de gestión de riesgos que está conformado por cuatro fases.

Figura 7.
Fases de la Gestión de Riesgos



Como todo proceso la gestión de riesgos se lleva a cabo cumpliendo un conjunto de actividades que están relacionadas entre sí y enfocándose desde la perspectiva de seguridad de la información y por qué no, cuando evaluamos o auditamos un sistema.

El proceso de gestión de riesgos ayuda a una organización a la toma de decisiones en torno a la seguridad de la información y por ende ayuda a alcanzar los objetivos estratégicos de la misma. Por ejemplo, una organización se puede dar cuenta que sus servidores no tienen un *firewall* de seguridad y tomar la decisión de implementarlo como para asegurar su información de posibles ataques de ciberdelincuentes. En torno a los riesgos la organización también puede tomar decisiones enfocadas en:

- Aceptar el riesgo en caso de que el impacto no sea muy grave al materializarse la amenaza.
- Implementar contramedidas o medidas para el tratamiento del riesgo en el sentido de mitigarlo o eliminarlo.
- Transferir el riesgo. Un ejemplo es cuando la organización contrata algún tipo de seguro, en caso de que la amenaza se materialice, otra empresa lo asume.
- Evitar el riesgo evaluando e identificando los controles o contramedidas que ayudarían a evitarlo, también se considera identificar los procesos o actividades asociadas al riesgo.

Algunas preguntas que ayudan a trazar la ruta para empezar con el proceso de gestión de riesgos son:

- **¿Cuáles son los peores escenarios en los que el sistema de información o los activos de información de la organización estén expuestos y en el peor de los casos sufran daños graves?** Para responder esta pregunta es necesario que identifiquemos los activos que queremos resguardar y en qué casos los riesgos se pueden materializar.
- **¿Cuán frecuente es que el riesgo se materialice?**
- **¿Cuánto es el daño que se produce en la organización cuando se materialice el riesgo?** Podemos cuantificarlo incluso en términos de costos.

Las preguntas anteriores nos pueden ayudar al análisis y evaluación de los riesgos como tal, pero para ya entrar al tema de tratamiento de estos es importante considerar:

- ¿Cómo se pueden tratar estos riesgos? En términos de verificar los controles y contramedidas necesarias, incluyendo los recursos que se necesitarán, creación de políticas, normas y procedimientos.
- Existan o no existan estos recursos, ¿cuánto le va a costar a la organización la implementación de controles? Tomando en cuenta también términos de tiempo.
- ¿Es rentable la implementación de controles? El análisis de coste/beneficio.

Algunos controles que se definen dentro de la gestión de riesgos son del tipo:

- Controles generales, administrativos y físicos, desde la creación de las políticas de seguridad, procedimientos para cumplir con objetivos de control.
- Controles proactivos conocidos más como salvaguardas y que procuran ser siempre proactivos.
- Controles correctivos, cuando los controles preventivos no han funcionado y de alguna manera queremos que lo que está afectado por algún evento, vuelva a la normalidad, se los conoce como controles reactivos.

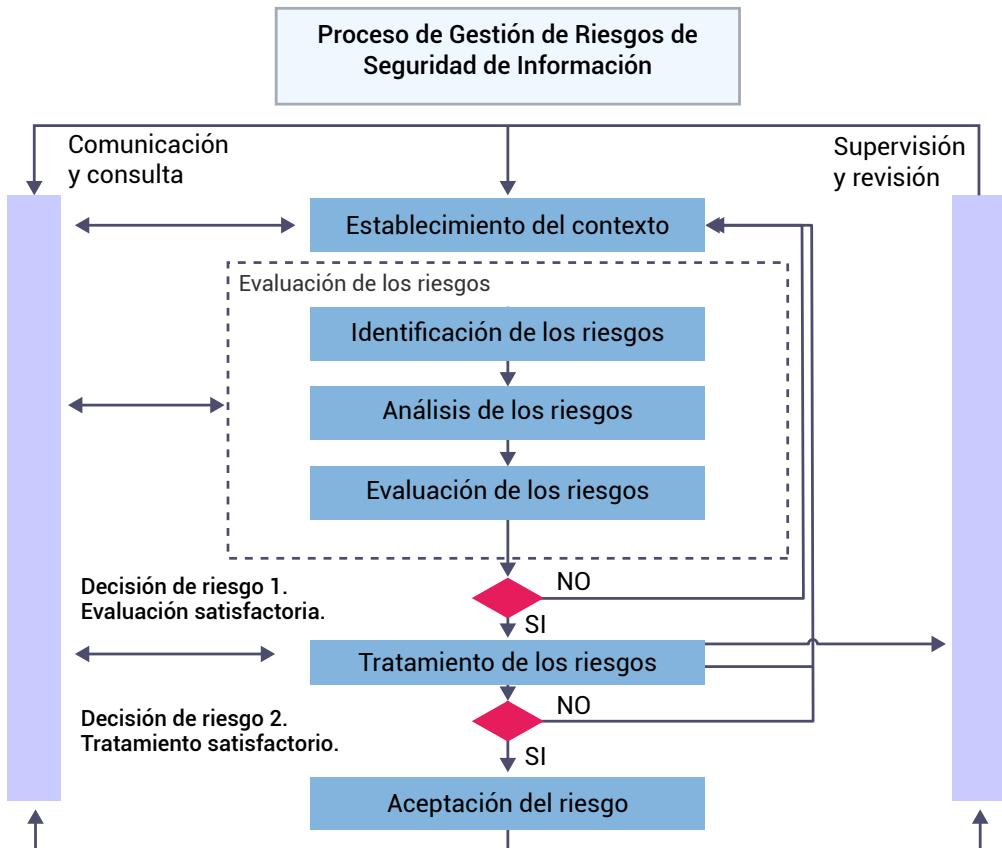
Independientemente de si se utiliza una buena práctica, norma o marco de referencia para realizar una adecuada gestión de riesgos, el proceso en sí enmarca las siguientes fases:

- Contexto de la gestión de riesgos
- Identificación del riesgo
- Análisis del riesgo
- Evaluación del riesgo
- Tratamiento del riesgo
- Comunicación del riesgo
- Monitoreo del riesgo

En la figura 8 podemos visualizar el proceso de la gestión de riesgos basado en la ISO 27005:

Figura 8.

Proceso de gestión de riesgos



Nota. Adaptado de REDCEDIA (2014). Gestión del riesgo de las TI ISO NTC 27005.

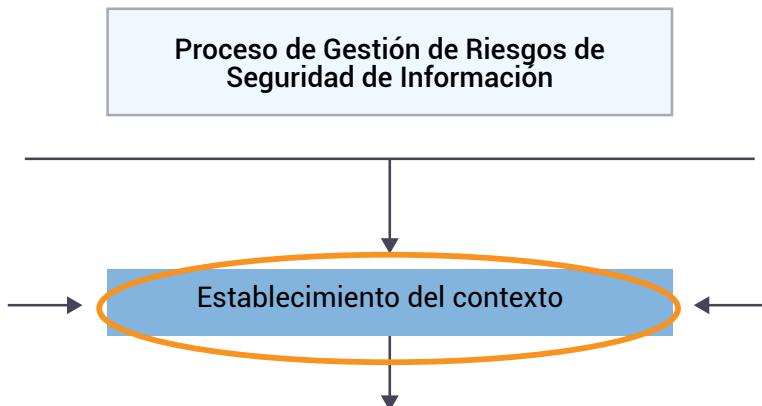
Para comprender mejor el proceso de gestión de riesgos, nos basaremos en la figura 8 antes descrita y se irá describiendo cada uno de estos apartados.

2.2. Contexto de la Gestión de Riesgos

Es el primer paso que se debe llevar a cabo para empezar con el proceso de gestión de riesgos. Para la explicación de este proceso vamos a tomar como base la figura 9.

Figura 9.

Establecer el contexto de la gestión de riesgos



Nota. Adaptado de REDCEDIA. (2014). Gestión del riesgo de las TI ISO NTC 27005.

Para (ISOTools, 2021) establecer el contexto es conocer todos los factores internos y externos que intervienen en la gestión de las organizaciones, identificarlos, analizarlos y comprenderlos para poder así llegar a la evaluación adecuada de los riesgos para así determinar cómo se dará respuesta a los mismos, cabe mencionar que a partir de esta evaluación de riesgos usted puede también determinar el análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) de la organización.

Según la ISO 31000 estos factores internos o externos pueden ser:

- Factores internos, como:
 - Cultura organizacional, gobierno, políticas, objetivos, sistemas de información, procedimientos, normas, etc.
- Factores externos, como:
 - Ambientales, cultura, gobierno, obligaciones legales y políticas, economía, mercado, competencia, etc.

La primera actividad para establecer el contexto es el levantamiento de información, como conocer la razón de ser de la organización, sus objetivos estratégicos, la misión y visión que la orientan, los productos o servicios que ofrecen, personal, cultura organizacional, socios o proveedores y también entender cuál es el propósito de una gestión de riesgos. Entre estos propósitos se puede destacar, por ejemplo, que la organización quiere

establecer un SGSI, busca una certificación, ha definido establecer un plan de continuidad de negocios o de respuesta a incidentes o establecer un proceso de contingencia.

Cuando ya se conoce el contexto de la organización se define el alcance de gestión de riesgos que nos ayuda a determinar los límites, como áreas que cubrirá este proceso de gestión de riesgos, es decir, la identificación, el análisis, evaluación y tratamiento de los riesgos puede ser solo en el área de procesamiento de datos o más conocido como CDP (Centro de Procesamiento de Datos) o también puede ser en toda la organización, esta decisión depende de la alta gerencia.

2.2.1. Definición del alcance de la gestión de riesgos

El definir el alcance de la gestión de riesgos se refiere a determinar el propósito o la razón del por qué se hará el proceso de la gestión de riesgos y se lo hace dentro del establecimiento del contexto de la organización, porque se necesita tener toda la información de la organización para que este alcance sea definido con claridad y se conozca incluso las limitaciones que pueden de alguna manera afectar indirectamente al implementar el proceso de gestión de riesgos. Por ejemplo, puede ser que la organización tenga restricciones con respecto a tecnología, financieras o quizás en cuanto a cultura organizacional, etc.

Dentro del alcance se considera también los criterios con los que evaluará el riesgo, es decir, ciertos eventos, documentos, procesos que ayudarán a dar valor al riesgo o que nos ayudarán a darnos una pauta para cuando se haga el tratamiento de estos. Como uno de estos criterios de evaluación se debe considerar también el impacto, es decir cuantificar (de manera financiera en lo posible) el daño de los activos de la organización, si en algún momento llegara a materializarse una amenaza por la existencia de una vulnerabilidad. Algunos puntos para tomar en cuenta el impacto pueden ser: cuánto afectaría el evento a los pilares de la seguridad de la información que son la confidencialidad, integridad y disponibilidad. Otro puede ser, cuánto en tiempo y en dinero la organización invierte para restablecer sus procesos principales en caso de que hayan sido interrumpidos y la probabilidad de cuantas veces puede materializarse una amenaza. En los siguientes apartados de la unidad 2 de este texto guía se estudiará más detalladamente los conceptos de impacto y probabilidad.

Al final de esta definición de alcance se plasmarán los objetivos que se quieren lograr con este proceso de gestión de riesgo, tomando en cuenta que sean objetivos claros y alcanzables en el tiempo.

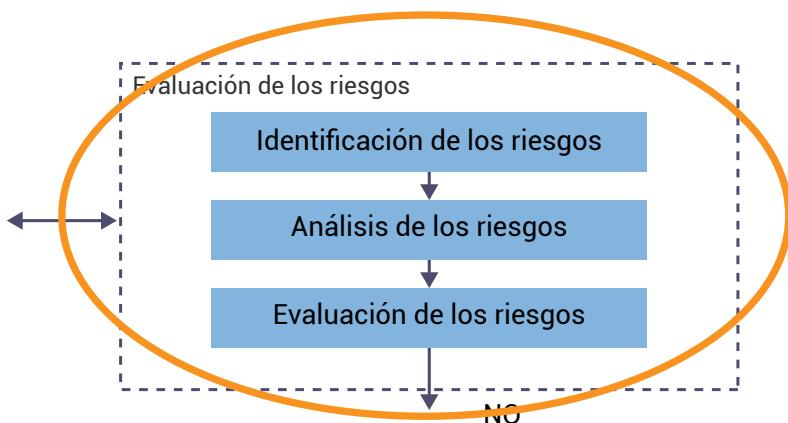
2.3. Proceso de análisis del riesgo

Las actividades que se desarrollan dentro de este proceso son algunas, que parten cuando se tiene claro el contexto de la gestión de riesgo estudiado en el apartado anterior.

Para hacer un análisis de riesgos adecuado es importante que la organización conozca los principales riesgos o amenazas a los que están expuestos sus principales activos. Enlistar e identificar los riesgos será el primer paso para poder hacer una correcta valoración y tratamiento de estos. En la figura 10 se describe el proceso de evaluación de riesgo.

Figura 10.

Proceso de Evaluación de riesgos



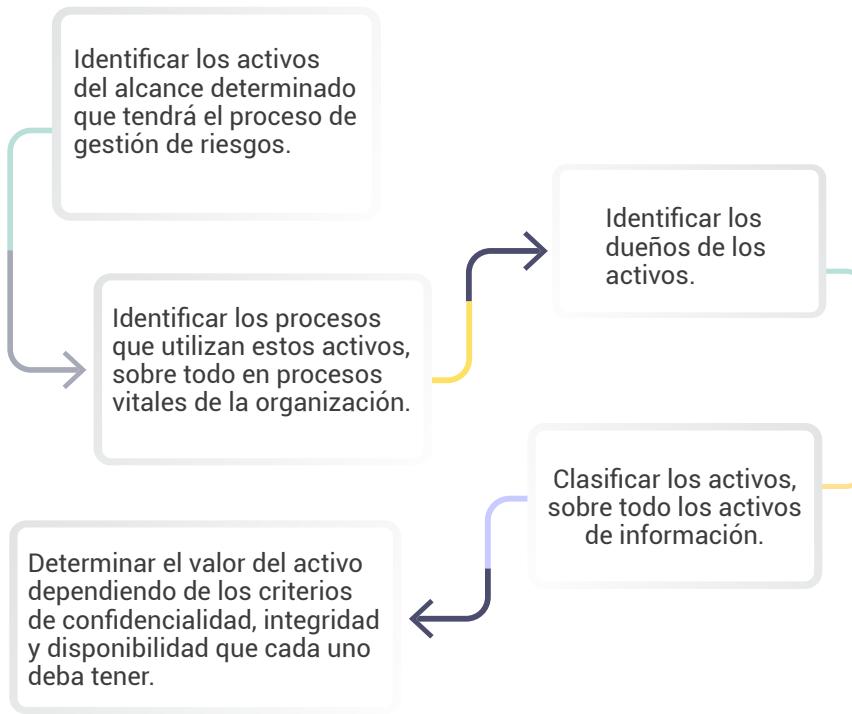
Nota. Adaptado de REDCEDIA. (2014). Gestión del riesgo de las TI ISO NTC 27005.

La identificación de riesgos empieza con la identificación las posibles fuentes de riesgos, sus causas y consecuencias.

Algunas fuentes de riesgos no se pueden identificar a simple vista, es por esto que es buena práctica empezar por *identificar los activos*, luego identificar las amenazas a los que estos están expuestos y las vulnerabilidades que estos tienen (utilizando ciertas herramientas atomizadas), como los controles existentes que quizás fueron ya

implementados en alguna ocasión; y, finalmente saber cuánto afectará esta amenaza al activo (impacto) tomando en cuenta la probabilidad de ocurrencia, para finalmente evaluar este riesgo, sacar su valor en una matriz de riesgos y priorizar su tratamiento. En la figura 11 se describe el proceso de identificación de activos y seguidamente se describe algunas actividades dentro de este proceso.

Figura 11.
Proceso de identificación de activos



2.3.1. Identificación de activos

La organización posee un conjunto de activos que son de mucho valor. Pueden ser todos los recursos que de alguna manera necesita para el día a día de sus funciones y por lo que siempre buscará resguardarlos. Una vez que se tiene el contexto de la gestión de riesgos, claramente los objetivos que se quiere lograr con ella y en donde se implantará, el siguiente paso es identificar cada uno de los activos detalladamente, que identifique en primer lugar al activo, que se sepa que es o que finalidad tiene dentro de la organización, cuál es el proceso en el que está involucrado y sobre todo el responsable de este activo.

Lo que se obtiene de esta identificación es una lista de activos con un valor prioritario para la organización que busca proteger. Existe una clasificación basada en la ISO 27005 que es importante considerar:

- *Activos primarios* se refiere a los procesos o actividades del negocio y una manera de identificarlos es mediante entrevistas al personal involucrado con estos principales procesos de negocio, como pueden ser personas especialistas en ciertas áreas del sistema de información. Los procesos y actividades de negocio son actividades que si existe alguna eventualidad se ven interrumpidas y de alguna manera afecta el desarrollo normal de la organización (o del negocio).

Dentro de cada proceso de negocio se maneja información. Puede ser información vital que es la entrada o salida del proceso como tal; como, por ejemplo, información de carácter personal.

- *Activos de soporte e infraestructura* son los activos que permiten de alguna manera que la información sea procesada y que son el soporte, como su nombre mismo lo dice, para que los procesos y actividades de negocio puedan funcionar. Por ejemplo, se puede identificar activos tipo *software*, *hardware*, redes, estructura física, servicios cloud, etc. (Martínez & Garzón, 2018).

Existen otras maneras de clasificar los activos, según (Interpolados, 2020), hoy en día la mayoría de las organizaciones tiene activos de TI. Es aconsejable que se maneje una gestión de activos de TI para tener la información precisa de lo que existe como recurso (*hardware*, *software*, servicios, etc.) dentro de la empresa. También se puede dividir la clasificación de estos activos de la siguiente manera:

- Activos de hardware
- Activos de software
- Activos de servicios en la nube
- Activos del cliente
- Activos de información

Una vez identificados los activos más importantes de la organización, se procede a valorar estos activos. Para valorar los activos sobre todo en cuanto a información se debe identificar el valor en cuanto a los tres pilares fundamentales de la seguridad de la información: Disponibilidad, Confidencialidad y Disponibilidad.

Valor del activo con respecto a disponibilidad. – Valoramos y clasificamos los activos de acuerdo con cuanto la organización requiere su disponibilidad, no todos los activos deben estar disponibles, pero habrá algunos, los más importantes que si deban. Se tomará de ejemplo los criterios de valoración de activos dados por (SISTESEG, 2018) ver la tabla.

Tabla 7.

Criterios para el nivel de disponibilidad de los activos

	Valoración de los activos			
	Mínimo (1)	Medio (3)	Grave (5)	Catastrófico (7)
Las pérdidas Económicas por indisponibilidad del activo son:	Mínimas	Media	Graves	Totales
Los servicios prestados se ven afectados por la indisponibilidad activo de la siguiente forma:	Interrupción leve o nula en suministro de servicios.	Obliga al cliente a cambiar de proveedor de forma transitoria.	Pérdida de algunos clientes de forma definitiva.	Pérdida de clientes clave.
La indisponibilidad del activo afecta la operación así:	Retrasos en funciones no vitales	Retrasos leves en funciones vitales.	Retrasos graves en funciones vitales.	Interrupción inmediata de funciones vitales.
La indisponibilidad del activo afecta la imagen en el sentido que:	No afectar la confianza en los productos o servicios.	Pérdida de confianza en un servicio específico o en una parte de la organización.	Pérdida de confianza de parte de los clientes	Pérdida de confianza del mercado y daños a la imagen de marca.
La indisponibilidad del activo afecta el cumplimiento de obligaciones en el sentido que:	Produce una falta leve en el cumplimiento de algún contrato.	Produce una falta en el cumplimiento de algún contrato que obliga a renegociar.	Produce una falta grave en el cumplimiento de algún contrato.	Deja a la organización al margen de la ley.

Nota. Tomado de SISTESEG. (2018). Metodología de análisis de riesgo según ISO 27005 :2018 e ISO 31000 : 2018.

Valor del activo con respecto a confidencialidad. – El nivel de confidencialidad se lo medirá basándose en la clasificación que utiliza la organización para clasificar la información. Puede ser como se muestra en la tabla 8.

Tabla 8.

Criterios para valorar la confidencialidad del activo

Clasificación	Valor
Pública	5
Uso interno	10
Confidencial	15
Reserva	20

Valor del activo con respecto a integridad. – El nivel de integridad se lo mide determinando que el mayor valor tendrá cuando ha alterado el activo de alguna manera y ocasiona grandes daños a la organización. Por ejemplo, la escala de valoración puede ser como se muestra en la tabla.

Tabla 9.

Criterios para valorar la integridad de un activo

Clasificación	Valor
Pública	5
Uso interno	10
Confidencial	15
Reserva	20

Para finalizar este proceso de valoración lo que se hace es sumar todos los valores y utilizar una escala para determinar el valor general. En la siguiente tabla se puede observar un ejemplo de escala de valoración de activos según (SISTESEG, 2018).

Tabla 10.

Valoración de activos por CID (Confidencialidad-Integridad-Disponibilidad)

VALORACIÓN DE ACTIVO	SUMATORIA DE LOS FACTORES CONSIDERADOS
MB: muy bajo	De 14 a 24
B: bajo	De 25 a 35
M: medio	De 36 a 46
A: alto	De 47 a 57
MA: muy alto	De 58 a 68

Nota. Tomado de SISTESEG. (2018). *Metodología de análisis de riesgo según ISO 27005:2018 e ISO 31000: 2018.*

Una vez valorados los activos se hace la identificación de amenazas en los activos como se describe en el siguiente apartado.

2.3.2. Identificación de amenazas en los activos

Una vez identificados y valorados los activos de la organización se procede a identificar las amenazas como inicio de empezar con la identificación de los riesgos. Las acciones principales para llevar a cabo esta actividad son:

- Revisar situaciones pasadas en donde los activos estuvieron amenazados o de incidentes en los que afectó de alguna manera el activo, siempre y cuando esto haya sido documentado.
- Toda amenaza tiene un origen. Es importante conocer este origen, de donde procede o por qué se podría de alguna manera materializar, es decir, posibles escenarios en los que estas amenazas se materializarían.

Las fuentes de la amenaza son aquellos agentes internos o externos que de alguna manera afectan los activos de la organización, sobre todo a nivel general. Ocasionan pérdidas o impide de alguna manera u otra alcanzar los objetivos de la organización. Con la lista de activos, uno a uno se va cuestionando si existen o no amenazas que los afecten, cuáles son, la probabilidad de que ocurran e incluso el impacto (daño) que ocasionan. Algunas fuentes pueden ser:

- Empleados descuidados.
- Falta de concienciación de las políticas de seguridad organizacionales.
- Uso de TI y desconocimiento del funcionamiento de estas.
- Si se tiene servicios externos como servicios en la nube es 100% probable que se sufra ataques de *hacker*.
- Contraseñas débiles.
- *Firewalls* mal configurados.
- Exposición a virus, etc.

Las herramientas utilizadas para identificar las amenazas y sus fuentes son entrevistas, observaciones del funcionamiento de los sistemas, revisión histórica de incidentes, utilizar quizá un cuestionario o *checklist* basado en una buena práctica (ISO 27001, 27002, COBIT ITIL) para ir descartando ciertas amenazas. Todo esto en todos los niveles de la organización desde gerencia hasta el personal técnico y usuarios finales. Se debe considerar que una amenaza puede afectar a más de un activo y un activo también puede estar expuesto a más de una amenaza.

2.3.3. Identificación de controles existentes para asegurar activos

Las fuentes de amenazas para los activos ya están identificadas en todo este proceso de gestión de riesgos, lo siguiente a estudiar es si de alguna manera fueron ya tratadas con algunos controles para evitar que la amenaza se materialice o tratar que si en caso sucede su impacto no cause demasiado daño a la organización.

Aquí se debe verificar la existencia de políticas, procedimientos, controles establecidos como: antivirus, control de accesos, copias de seguridad, etc. Cuando se verifica y se conoce los controles existentes, cuando se haga el tratamiento del riesgo, la organización evitará volver hacer procesos ya establecidos y proponer controles ya implementados y con ello ahorrará costos. Informes de auditorías hechas con anterioridad serán muy valiosas para esta actividad y si no hay la suficiente documentación se recomienda lo siguiente:

- Entrevistas con los responsables de la seguridad de la información.
- Entrevistas con usuarios para verificar la funcionalidad de controles establecidos.
- Análisis de la información de documentación de controles implementados.
- Cuestionarios y listas de verificación.

Dentro de los controles establecidos para el tratamiento del riesgo, algunos no funcionan, por lo tanto, deben ser igual evaluados para corregirlos cuando se haga el tratamiento del riesgo.

2.3.4. Identificación de vulnerabilidades

(Romero Castro et al., 2018) se refiere a la vulnerabilidad como un fallo en el diseño de procedimientos o de los activos de una organización, así como afirma que las vulnerabilidades existen, no se fabrican. Teniendo presente esta definición se debe hacer una evaluación en algunas áreas de la organización, sobre todo en los procesos y procedimientos, operaciones diarias, recursos humanos y recursos físicos, infraestructura en general.

Con las amenazas claras e identificadas para los activos y el estudio de controles existentes, se tendrá la lista de vulnerabilidades que pueden ser explotadas por estas amenazas para materializarse. No solo basta con tener esta lista de vulnerabilidades, sino que se debe estudiar estas vulnerabilidades en todos los posibles escenarios en los que se podría

explotar esta vulnerabilidad, con ello se podría hacer una combinación de controles, preventivos, correctivos o defectivos.

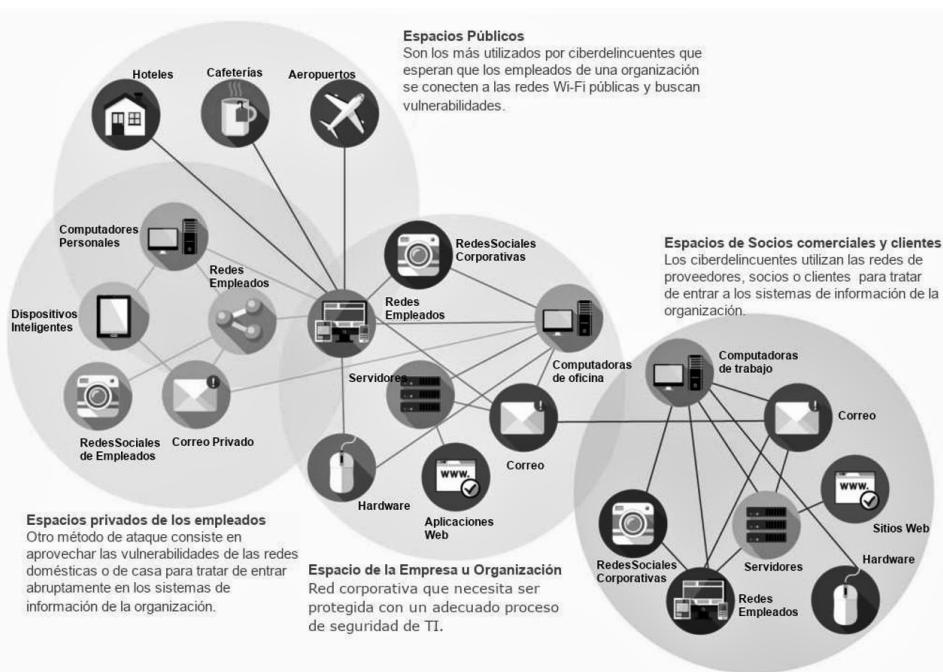
Es importante identificar las vulnerabilidades del sistema de información de la organización, tanto interna como externamente. Las vulnerabilidades internas pueden estar enfocadas, por ejemplo, en la parte de proceso de aseguramiento. Por ejemplo, qué tan claras y conocidas son las políticas, procedimientos y controles de seguridad. En las vulnerabilidades externas es un poco más amplio enfocarse en analizar toda la infraestructura, sobre todo la infraestructura crítica que es de apoyo y soporte para los procesos críticos de negocio de la organización. Entonces es aquí donde la superficie de ataque es más grande, pues hay que tomar en cuenta que la mayoría de las organizaciones hoy en día forman parte del ciberespacio. En la figura 12 podemos visualizar una estructura de superficie de ataque.



Para afianzar más este tema es importante que usted desarrolle la actividad 4 propuesta al finalizar esta semana, donde se abordará el tema de explorar bases de datos de vulnerabilidades.

Figura 12.

Estructura de superficie de ataque



Nota. Tomado de Superficie de Ataque Cibernético. (2016). [Gráfico]. https://graquantum.com/wp-content/uploads/2016/07/CyberAttackSurface_blogGraphic_Lindsay-1024x790.jpg

Para (Romero Castro et al., 2018) se pueden analizar algunas superficies de ataque para identificar amenazas estas son: software, hardware y los recursos humanos.

Software. - Son vulnerabilidades que se pueden encontrar en aplicaciones y servicios, como FTP, SSH, TELNET, etc. Los ataques pueden aprovechar vulnerabilidades como puertos abiertos en los servicios, errores de programación en las aplicaciones Web, fallos del sistema, configuraciones de software mal hechas. Una buena práctica frente a los accesos, a los sistemas se considera la ley de mínimos privilegios y utilizar software de fuentes confiables.

Para profundizar el tema de vulnerabilidades de software es importante que revise usted el [Top Ten de vulnerabilidades de OWASP](#).

Hardware.- Son vulnerabilidades de los dispositivos físicos. Puede ser porque el hardware está obsoleto o porque los equipos no están seguros, sobre todo de desastres naturales. Los ataques más comunes que se suelen tener son por medio de la red y afecta a la transmisión de datos y también como lo menciona (Romero Castro et al., 2018) en las comunicaciones de sistemas de alarmas o sensores. Otro ejemplo claro son las vulnerabilidades que hoy en día existen en el uso de nuevas tecnologías como el IoT (Internet de las cosas). Para reducir estas vulnerabilidades, se lo hace mediante instalaciones seguras y controles de acceso. Se debe tener cuidado sobre todo de puertos abiertos innecesariamente y de protocolos de comunicación no seguros, los firewalls: sistemas de detección de intrusión y sistemas de balanceo de carga son algunos controles eficientes en algunos casos.

Para profundizar el tema de vulnerabilidades de hardware es importante que revise usted las vulnerabilidades de IoT (internet de las cosas) que se detallan en el siguiente enlace: [Top Ten vulnerabilidades IoT](#)

Recursos humanos. - son las fuentes de vulnerabilidades que menos se puede controlar, ya que es el eslabón más débil de la ciberseguridad y que puede actuar en contra de la organización por varios motivos, descontento, engaño, soborno, etc. Tener un registro de actividades o una matriz donde se incluya las responsabilidades de lo que hace cada uno dentro de la organización. La verificación cada cierto tiempo ayudará a dar seguimiento de las responsabilidades. Otra buena práctica es dar de baja a usuarios o personal que ya no es miembro de la organización.

Para profundizar el tema de vulnerabilidades con respecto a recursos humanos, revise en el siguiente enlace [cómo se puede cambiar las malas prácticas de las personas respecto a la seguridad de información.](#)

El equipo encargado de identificar las vulnerabilidades tiene como apoyo algunas herramientas automáticas y semiautomáticas para poder identificar vulnerabilidades, lo importante aquí es tener claro que estas herramientas pueden dar falsos algunos resultados en tipo informe los cuales pueden contener falsos negativos, falsos positivos y verdaderos negativos. Como buena práctica se aconseja utilizar más de una herramienta para verificar estos resultados. Estas herramientas se conocen como pruebas

de seguridad de aplicaciones denominadas: SAST (Pruebas de seguridad de aplicaciones estáticas), DAST (Pruebas de seguridad de aplicaciones dinámicas) y las IAST (Pruebas de seguridad de aplicaciones interactivas).

Para profundizar el tema de pruebas de seguridad de aplicaciones puede revisar el siguiente enlace: [Diferencias entre SAST, DAST, IAST y RAST](#).

2.4. Proceso de evaluación del riesgo

En el proceso de análisis de riesgo se identifican los activos y los riesgos a los que están expuestos y el proceso de evaluación de riesgos es hacer los cálculos necesarios de la probabilidad en que el riesgo se materialice y el impacto que tiene en la organización, dando como resultado final el valor del riesgo. Esta actividad es conocida como estimación del riesgo. Cuando se determina el valor del riesgo, esto nos ayudaría a priorizar los riesgos para poderlos tratar.

Para la estimación del riesgo se utilizan ciertas metodologías; pueden ser cualitativas o cuantitativas, para identificar tanto el impacto como probabilidad de ocurrencia.

Le invito a profundizar sus conocimientos acerca de este importante tema:

2.4.1. Identificación de impacto

Es la actividad de verificar cuánto se afectará la organización si se materializa el riesgo o la amenaza, las pérdidas no solo se ven afectadas en torno a lo económico y materiales sino también en otros ámbitos. Existen algunos puntos a considerar como consecuencias de que se materialice el riesgo. Ver tabla 11.

Tabla 11.*Consecuencias de la materialización de riesgo*

Resultados del impacto de los riesgos	La pérdida de eficacia en el funcionamiento operacional de los sistemas;
	La inestabilidad en el funcionamiento de sistemas;
	Condiciones adversas de operación;
	Pérdida de la oportunidad de negocios;
	Imagen y reputación afectadas;
	Violación de obligaciones reglamentarias;
	Pérdidas financieras;
	La pérdida de datos e información;
	La pérdida de vidas humanas;
	Pérdida de competitividad
	Entre muchos otros, de acuerdo con los negocios de la organización.

Nota. Tomado de REDCEDIA. (2014). Gestión del riesgo de las TI ISO NTC 27005.

Anteriormente se ha mencionado que es bueno basarse en escenarios para evaluar los riesgos, no solamente para ver el valor real del riesgo como tal, sino, el impacto, daño o consecuencia que se generaría cuando se materialice en ciertas condiciones. En donde para estos escenarios se necesita identificar los actores que intervienen, el tipo de amenaza al que está expuesto el activo, la acción que materializa el riesgo o que hace que este ocurra, contra qué clase o tipo de activos afecta (impacto) y en qué tiempo o durante qué tiempo ocurrirá o cuantas veces (probabilidad).

El impacto puede ser medido en torno a la pérdida o degradación de la disponibilidad de los activos, la pérdida de la confidencialidad o la pérdida de integridad o como se vio en apartados anteriores, la pérdida total del activo, para esto es necesario que se tenga la identificación clara de activos, su valor, sus vulnerabilidades y los controles impuestos en los mismos.

La primera tarea a realizar para poder medir el impacto es de la lista de activos identificados en la organización, ordenarlos y de acuerdo con su valor ver su criticidad, es decir, cuáles son los que se debe resguardar o proteger. Según (REDCEDIA, 2014) es posible hacer esto de las siguientes maneras:

- Determinación del costo financiero de reposición o recuperación del activo y todo lo que él posea (información). De aquí que el valor de los activos está directamente relacionado con el valor del impacto.
- Determinación del valor por el impacto a procesos críticos del negocio.

Utilizar una metodología de análisis cualitativo para estimar el riesgo, significa que se usará atributos calificadores y descriptivos, pero no se utiliza el valor del costo del activo. Como será una estimación muy subjetiva, lo que se aconseja es su uso al inicio cuando se quiere determinar el contexto de la gestión de riesgos y aún no se tiene suficiente información. En la figura 13 se determinan algunos ejemplos de valores cualitativos para estimar el impacto.

Figura 13.

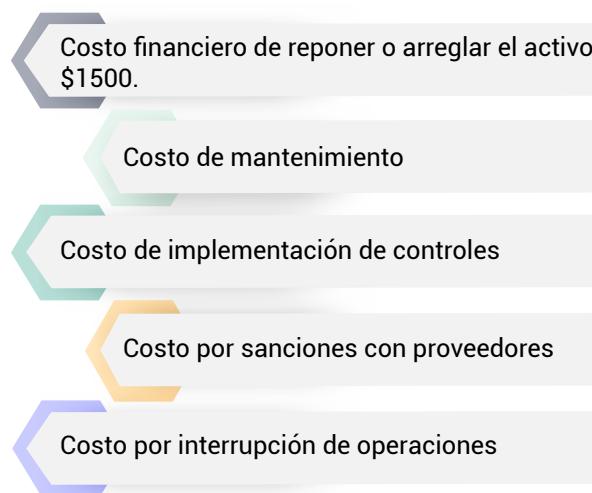
Valores cualitativos para estimar el impacto



En la mayoría de los procesos de evaluación de riesgos se utiliza una metodología cuantitativa, es decir, valores numéricos para estimar el impacto. Se utiliza este tipo de metodología cuando se puede estimar los valores o costos financieros de los activos. Esta metodología también se basa en datos históricos o de auditorías anteriores. En la figura 14 se exemplifica como se puede estimar el impacto a nivel cuantitativo.

Figura 14.

Valores cuantitativos para estimar el impacto



Otra opción es utilizar valores numéricos para luego, cuando se valore el riesgo, sea más fácil sacar el resultado final, en la siguiente tabla se describe:

Tabla 12.

Valores numéricos

Valor cuantitativo	Valor cualitativo
5	Grave
4	Medianamente Grave
3	Limitado
2	Medianamente Limitado
1	Ligero

2.4.2. Identificación de la probabilidad

La evaluación de la probabilidad tiene que ver con cuán probable es la ocurrencia o la materialización de la amenaza o riesgo. Para esto es importante que el equipo de análisis de riesgos se base en información de indicadores o variables identificados de incidentes que han pasado con anterioridad. Existen tres puntos a considerar para estimar la probabilidad, estos son:

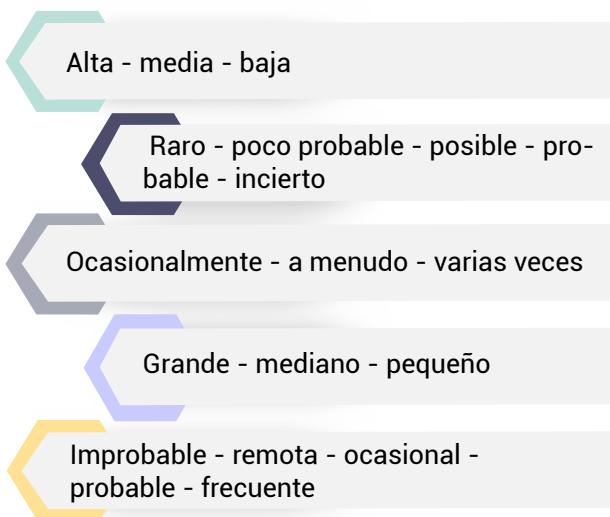
- Estudio del historial de ocurrencias.

- La frecuencia de ocurrencia de las amenazas, tomando en cuenta las intencionales y las accidentales.
- Facilidad con la que las vulnerabilidades pueden ser explotadas.

Estos 3 puntos son basados en las posibles vulnerabilidades encontradas, identificadas o estudiadas de cada uno de los activos. La materialización de las vulnerabilidades debe ser estudiada individualmente, al igual que para estimar el impacto se utiliza metodologías cualitativas o cuantitativas (ver figura 15).

Figura 15.

Valores cualitativos para estimar la probabilidad



Al finalizar esta semana estará en capacidad de comprender los primeros lineamientos del proceso de gestión de riesgos, identificarlos, analizarlos para posteriormente evaluarlos y hacer un plan de tratamiento y dejar establecido un plan de contingencia con los contenidos que se desarrollan en los siguientes apartados. Se recomienda que refuerce conocimientos antes de empezar la siguiente unidad, para esto es importante que realice las actividades de aprendizaje recomendadas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

Lecturas en bibliografía básica, complementaria y recursos educativos abiertos

- Revise algunas consideraciones que se deben tener en cuenta para empezar el proceso de gestión de riesgos.
- Documento Gestión de Riesgos de TI (3. Gestión de Riesgo y 4. Análisis de Riesgo)
- Libro Introducción a la seguridad Informática y el Análisis de Vulnerabilidades – (Capítulo 2: Fundamentos de la ciberseguridad subtemas 2.1 Los tres pilares de la seguridad y 2.2 Evaluación de riesgos, amenazas y vulnerabilidades)
- Libro Fundamentos de seguridad informática (Unidad 3: Amenazas y sus tipos Vulnerabilidades, tipos y factores)

■ Actividad 1

Explore las siguientes bases de datos de vulnerabilidades. Identifique dos bases de datos con las que se familiarice y realice pruebas.

Base de Datos

[Vulnerability Database](#)

[National Vulnerability Database](#)

[Common Vulnerabilities and Exposures](#)

[Open Source Vulnerability Databases](#)

■ Actividad 2

Revise el siguiente enlace donde se muestra la [Diferencia entre las vulnerabilidades de hardware y software](#). Identifique una empresa en la que usted podría aplicar estas diferencias y enliste, 10 vulnerabilidades en cuanto a software que encuentre y 10 vulnerabilidades a nivel de hardware.

Resultado de aprendizaje 5

- Identificar las medidas cuantitativas y cualitativas que se pueden utilizar para evaluar el riesgo y evalúa la eficacia de las políticas y prácticas de gestión de riesgos en relación del costo/beneficio de su implementación.

Contenidos, recursos y actividades de aprendizaje

Las organizaciones al decidir implementar un proceso de seguridad basado en una adecuada gestión de riesgos necesitan utilizar una herramienta de gestión que permita determinar objetivamente estos riesgos y se la conoce como *Matriz de Riesgos*. Es una herramienta sencilla de entender y utilizar una vez comprendidos los conceptos básicos y fundamentales estudiados hasta ahora, pero sobre todo comprender la probabilidad de que una amenaza se materialice y cuán dañino puede ser su impacto en la organización, utilizando ambas valoraciones para poder estimar el riesgo. Ahora, ¿Cómo valoramos el riesgo? ¿Cómo lo tratamos? ¿Cómo se implementa el proceso de gestión de riesgos? La respuesta es mediante la matriz de riesgos.



Semana 4

2.5. Valoración del riesgo – Matriz de riesgo

Para estimar el valor del riesgo se utilizará una fórmula matemática **Riesgo = Impacto x Probabilidad**, cuyos resultados se presentan incluyendo una clasificación de su criticidad de estos por colores, el gráfico de resultados se representaría como la tabla 13.

Tabla 13.*Ejemplo de matriz de riesgo*

Matriz de Riesgos		Puntuación de probabilidad por impacto				
Probabilidad		Impactos				
		Muy baja	Baja	Media	Alta	Muy alta
Muy alta	5	9	18	36	72	
Alta	4	7	14	28	56	
Media	3	5	10	20	40	
Baja	2	3	6	12	24	
Muy baja	1	1	2	4	8	

Existen algunas herramientas para poder generar este tipo de matrices, como por ejemplo [Primavera Risk Analysis Tool](#), o, se puede utilizar alguna plantilla de las muchas que existen desarrolladas en Excel o Word.



En la actividad 1 se pide desarrollar una actividad tomando en cuenta una matriz de riesgos y se enlistarán algunas matrices de riesgos para que escoja en cuál trabajar.

Como ya se ha mencionado la estimación de la probabilidad se define cuando el equipo de la gestión de riesgo está en la etapa del contexto. En la mayoría de los casos para evaluar riesgos en cuanto a seguridad de la información de una organización lo que se hace es utilizar el método cualitativo, es decir, crear escalas que sean igual a valores numéricos. Por ejemplo, en la tabla 14 está definida una escala de probabilidad que debe estar muy clara, antes de ser utilizada.

Tabla 14.*Escala de probabilidad*

Probabilidad	Probabilidad de ocurrencia %	Probabilidad de ocurrencia cuantitativa
Muy alta	Mayor al 80%	5
Alta	Entre el 51% y 80%	4
Mediana	Entre el 31% y 50%	3
Baja	Entre el 11% y 30%	2
Muy baja	Entre el 1% y 10%	1

La estimación del impacto al igual que la probabilidad se la define al inicio en el contexto de la gestión de riesgos o en algunos casos también se la

conoce como la etapa de planificación de este proceso. En este texto guía se estudió en un apartado anterior el impacto y cómo se lo identificaba. Recordemos que este puede ser en términos de daño o recuperación del activo, afectación a la calidad, o incluso quizá afectando los tres pilares fundamentales de la seguridad, integridad, disponibilidad y confidencialidad, etc. En la tabla 15 se ejemplifica la escala del impacto.

Tabla 15.

Escala de impacto al CID

Tipo de impacto	Muy Alto 5	Alto 4	Medio 3	Bajo 2	Muy bajo 1
Disponibilidad	Suministros de servicios interrumpidos totalmente	Interrupción casi total del suministro de servicios	Interrupción moderada del suministro de servicios	Interrupción leve del suministro de servicios	Interrupción nula del suministro los servicios
Integridad	Información modificada afecta mucho a la gestión operativa de la organización	Información modificada afecta moderadamente a la gestión operativa de la organización	Información modificada afecta parcialmente a la gestión operativa de la organización	Información modificada pero no afecta el sentido total de la gestión operativa de la organización	Información modificada no afecta en nada a la gestión operativa de la organización
Confidencialidad	Secreta	Reservada	Confidencial	Uso interno	Pública
Costo de Recuperación	Mayor a \$25000	De \$10000 a \$25000	De \$5000 a \$10000	De \$5000 a 2000	De \$2000 a \$1000
Calidad	No pasa los test de calidad	Tiene el 75% de rechazo en los test de calidad	Tiene el 50% de aceptación en los test de calidad	80% de aceptación de los test de calidad	95% de aceptación de los test de calidad

2.5.1. Escalas del apetito o tolerancia del riesgo

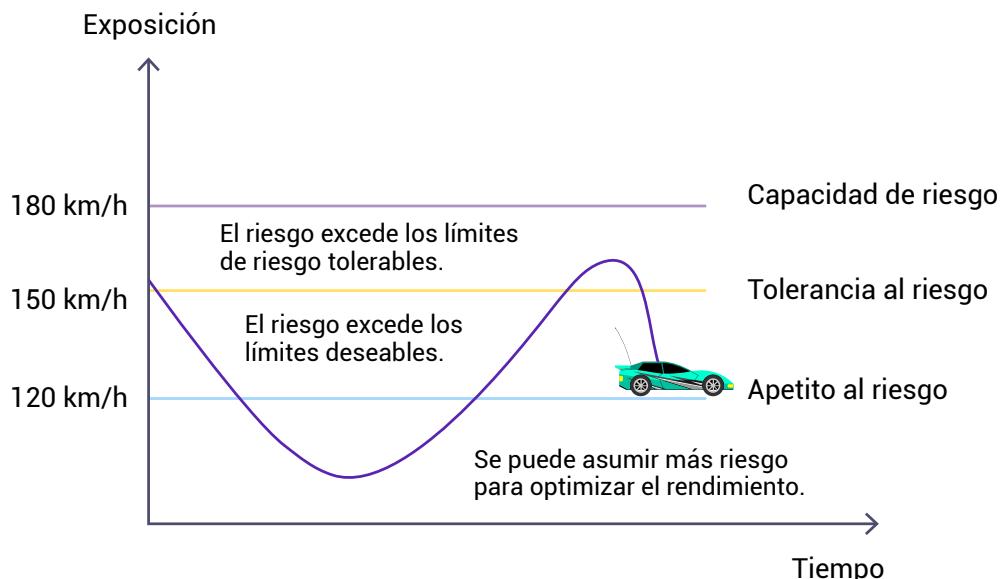
Ya se han determinado las escalas o las estimaciones de la probabilidad y del impacto, también se necesita la escala de apetito de riesgo o la escala de tolerancia. Dos conceptos nuevos que se deben conocer en este apartado:

- *Apetito de riesgo*: grado de incertidumbre en el que una organización está dispuesta a aceptar en previsión por una recompensa.
- *Tolerancia al riesgo*: es el grado de incertidumbre que la organización soportará.

Para entender estos conceptos se tomará de ejemplo la figura 16.

Figura 16.

Diferencia entre capacidad, tolerancia y apetito de riesgo



Nota. Tomado de <https://fraudeinterno.wordpress.com/2018/10/03/diferencia-entre-apetito-tolerancia-y-capacidad-de-riesgo/>

En este ejemplo se considera la *capacidad del riesgo* a la *capacidad* que tiene el vehículo de ir a 180km/h, pues fue creado para poder soportar esta velocidad. Sin embargo, supongamos que ese día el clima lluvioso hizo que la calzada esté húmeda y la experiencia del conductor de alguna manera no es muy buena en esas condiciones de clima, así que toleraría ir a 150km/h (*tolerancia al riesgo*). Sin embargo, para respetar el tiempo y no incumplir alguna ley de tránsito y sobre todo viajar de manera segura, decide que su velocidad sería de 120km/h (*apetito de riesgo*).

La tolerancia al riesgo depende de muchos factores, por lo que hoy en día no se la considera como un parámetro para la evaluación de riesgos; sin embargo, se puede utilizar la tolerancia o el apetito indistintamente. El determinar los niveles de apetito de riesgo nos ayuda a utilizar una codificación de colores que permitirá priorizar los riesgos. En la tabla 16 podemos observar cómo sería la determinación de los niveles de apetito de riesgo.

Tabla 16.

Niveles de apetito de riesgo

Apetito de riesgo	Color	Valor del riesgo
Alta	Rojo	Mayor o igual 15
Media	Amarillo	Mayor a 4 hasta 12
Baja	Verde	Menor o igual a 4

2.5.2. Esquema de valoración de la matriz de riesgos

Con la estimación de probabilidad, impacto y apetito de riesgo se procede a la creación de la matriz de riesgo y sobre todo la valoración que tendrá la misma. Se tomará los valores de impacto y probabilidad establecidos como:

- Probabilidad valores de 5, 4, 3, 2 y 1
- Impacto valores de 5, 4, 3, 2 y 1

Si se utilizaran valores no enteros se redondean los valores al entero más cercano. En algunos casos o situaciones se considera utilizar también valores exponenciales tomando en cuenta la realidad del caso, sobre todo calcular la magnitud de daños. Es por eso por lo que algunos equipos deciden utilizar por ejemplo exponenciales de 2. En la tabla 17 se muestra como quedaría la matriz de riesgos al multiplicar probabilidad por impacto.

Tabla 17.

Matriz de riesgos

Matriz de riesgo		Impacto				
Probabilidad		Muy bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy alto (5)
Muy alto (5)		4	10	15	20	25
Alto (4)		4	8	12	16	20
Medio (3)		3	6	9	12	15
Bajo (2)		2	4	6	8	10
Muy bajo (1)		1	2	3	4	5

Con esta matriz de valoración de riesgos ahora se tiene claras las zonas de priorización del riesgo y estas son:

- En rojo: riesgos de prioridad alta
- En amarillo: riesgos de prioridad media
- En verde: riesgos de prioridad baja

Si podemos recordar, para la estimación del impacto se realizó una matriz donde se tomaban en cuenta algunos indicadores para calcularlo. El valor final del impacto será el mayor. Por ejemplo, consideremos lo expuesto en la tabla 18:

Tabla 18.
Valor final del impacto

Código de riesgo	Nombre o descripción del riesgo	Impacto				
		Disponibilidad	Integridad	Confidencialidad	Costo de recuperación	Calidad
R001	Reutilización de un módulo desarrollado previamente	3	4	3	5	2
R005	Terremoto	5	5	5	5	1

El valor del impacto para el riesgo R001 es igual a 5.

Finalmente se genera los informes de la matriz de riesgo. Para generarlo, tomo datos de información real del registro de riesgos que se lo hizo cuando los identificamos. El registro de riesgos es un repositorio donde se registran los detalles de los riesgos individuales del proyecto junto con todos sus respectivos campos y se lo genera cuando se empieza a identificarlos.

Ahora se decide que herramienta utilizar, pero independientemente de la herramienta que se utilice, se tendrá una matriz como se muestra en la tabla 19.

Tabla 19.
Matriz de riesgo del ejemplo

Matriz de riesgo		Impacto				
Probabilidad	Muy bajo (1)	Muy bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy alto (5)
Muy alto (5)	4	10	15	20	25	
Alto (4)	4	Riesgo 004	12	Riesgo 001	Riesgo 005	
Medio (3)	3	6	9	12	Riesgo 007	
Bajo (2)	2	Riesgo 002	6	8	10	
Muy bajo (1)	1	2	3	4	5	

Al calcularse el valor del riesgo y al ubicarlo en la matriz en el ejemplo nos podemos dar cuenta que los riesgos *Riesgo 001*, *Riesgo 005* y *Riesgo 007* serían los tres principales riesgos de alta prioridad que hay que tratarlos, luego el de mediana prioridad *Riesgo 004* que, en su caso, igual habrá que tratarlo de alguna manera y finalmente el *Riesgo 002* que es un riesgo de prioridad baja en que la mayoría del caso la organización acepta el riesgo.

No se debe considerar la utilización de la matriz por una sola vez, es decir, una vez que se estableció el tratamiento de los riesgos de acuerdo con el informe arrojado por esta matriz, nuevamente se vuelve a hacer la estimación del riesgo considerando los controles que se implementaron para tratar los riesgos más altos y se regresa a la fase de identificación de riesgos de su impacto y probabilidad, mucho más si el equipo de gestión de riesgos se está basando en una buena práctica como la ISO 27005 basada en un ciclo de mejora continua.

Al final, cada vez que se trata el riesgo, su valor debe disminuir y su nivel de tratamiento bajar.

En algunas ocasiones también se utiliza otros parámetros para tener más claro cómo gestionar el riesgo, la facilidad con la que se puede tratar este riesgo denominado *capacidad del riesgo*, si es fácilmente tratable será establecida con el parámetro de fácil, si no, se la califica como difícil. Ejemplo de la tabla 20.

Tabla 20.

Capacidad del riesgo

Código de riesgo	Nombre o Descripción del Riesgo	Impacto					
		Disponibilidad	Integridad	Confidencialidad	Costo de recuperación	Calidad	Tratamiento
R001	Reutilización de un módulo desarrollado previamente	3	4	3	5	2	Difícil
R005	Terremoto	5	5	5	5	1	Muy Difícil

Se puede utilizar como ejemplo una lista con el detalle de cómo será se valorará el tratamiento (tabla 21).

Tabla 21.*Valorar la capacidad de tratamiento de riesgo*

Tratamiento	Descripción
Muy difícil	La organización prácticamente no se recupera.
Difícil	Requiere cambiar procesos críticos establecidos en la organización. El costo de tratamiento de este riesgo es muy alto.
Moderado	Requiere cambios moderados en los procesos de la organización. El costo de tratamiento es moderado.
Fácil	Requiere mínimos cambios para el tratamiento de riesgos. No habrá gastos

2.6. Proceso de tratamiento de los riesgos

Estimado el valor de riesgos ya se tiene una idea leve de cómo podríamos tratarlos, pero ¿Cómo identificamos los controles necesarios para tratarlos? ¿Qué consideraciones se deben tomar para saber la mejor manera de tratarlos?

Para empezar con el proceso de tratamiento debemos entender el tipo de tratamiento al cual serán sometidos los riesgos, según (Arteaga Martínez, 2017) estos son:

- Evitar el riesgo:** es cuando el equipo de análisis determina riesgos cuyo costo de tratamiento es mayor que los beneficios del propio servicio u organización. Lo que se procede hacer es eliminar la actividad o proceso que esté provocando el riesgo, en otras palabras, tratar de eliminar la fuente de riesgo.
- Reducir/Mitigar el riesgo:** medidas que se las considera para disminuir el riesgo, es decir, la probabilidad de que se materialice y si en caso se materializa, pues que su impacto sea el mínimo aceptado por la organización. Para reducir el riesgo se puede implementar controles para:
 - Corregir alguna anomalía
 - Eliminar errores y vulnerabilidades
 - Reducir el impacto cuando se materializa el riesgo.
 - Descubrir errores
 - Volver al curso normal (recuperación)
 - Monitoreo de vulnerabilidades, amenazas y riesgos

- Concienciación para orientar sobre la seguridad de la información
- c. **Transferir el riesgo:** son medidas tomadas para que la organización transfiera el riesgo a otra organización, el ejemplo más común es el contrato de seguros privados a los empleados o seguros de infraestructura que cubran de alguna manera las consecuencias o el impacto de un evento sucedido.
- d. **Asumir/Aceptar el riesgo:** en caso de que el riesgo fue reducido o transferido y exista un riesgo residual, debe recordar que no se puede controlar a veces el 100% de un riesgo; y, si según el equipo de gestión de riesgos, el impacto de este riesgo residual es el mínimo, pues la organización lo asumiría quizás con la creación de planes de contingencia o de aceptando la pérdida económica por lo residual.

Dentro de este proceso de tratamiento de riesgos lo que se hace es identificar y diseñar las opciones para tratar el riesgo, evaluar estas opciones y sobre todo ver la viabilidad de aplicabilidad de estas. En este punto el equipo de análisis también identifica los controles redundantes e innecesarios, posibles de quitarlos y para tomar la decisión de removerlos se debe conocer perfectamente que afectaría hacerlo, sobre todo el impacto sobre los activos en los que están implementados estos controles.

Para (Valencia-Duque & Orozco-Alzate, 2017) es importante tomar en cuenta que para hacer el plan de tratamiento de riesgos se haga el análisis de costo-beneficio de los controles que se van a implementar y el presupuesto que se consideró para su implementación. Es por esto la importancia de priorizar riesgos y para hacer este proceso se necesita empezar por un plan de tratamiento de los riesgos, aunque se prioricen los riesgos más importantes y el costo en tiempo y dinero cuesta mucho, mientras se los controla, se puede empezar a implementar los controles cuyo costo es más bajo y rápido.

2.6.1. Plan de tratamiento de riesgos

Para (Valencia-Duque & Orozco-Alzate, 2017) un plan de tratamiento de riesgos considera los siguientes puntos:

- Escenario del riesgo
- Riesgo residual

- Alternativa de tratamiento (recomendaciones)
- Controles a implantar
- Resultados esperados de los controles implementados
- Responsable de su implementación
- Costo estimado
- Fechas de implementación

Se puede crear una matriz donde irá el tratamiento de cada uno de los riesgos con la finalidad de tener un orden específico. Esta matriz será la herramienta que incluso se la utilizará en la etapa de monitorización para verificar si todo va como debería ir.

Desde el punto de vista de (Arteaga Martínez, 2017) el plan de tratamiento de los riesgos contempla el riesgo (escenario de riesgo), las recomendaciones de control que se sugieren aplicar para tratar el riesgo y se indica la priorización de las acciones que pueden ser: alta, moderada, media o baja. Se seleccionan los controles a aplicar de la lista de controles sugeridos, también se describen los recursos que se deben tener en cuenta para la implementación o aplicación de los controles seleccionados, se establece el o los responsables, así como el control de tiempo; y, de manera opcional se indican algunos comentarios u observaciones. En el siguiente documento se muestra un ejemplo de cómo se armaría el plan de tratamiento de riesgos. Ejemplo de tratamiento de riesgo.

Ejemplo de tratamiento de riesgo

Tal como se muestra en el ejemplo de la anterior figura se trabajan absolutamente con todos los riesgos identificados. Una vez concluida esta fase el equipo lo que debe hacer es determinar los riesgos residuales que son los que permanecen después de la implementación de los controles para evitar, transferir o mitigar los riesgos. La posibilidad que queda de ocurrencia del riesgo después de la implementación del control para mitigarlo caracteriza el riesgo residual. Es decir, son los riesgos restantes después de tomar medidas para evitarlos, transferirlos o mitigarlos.

Este riesgo residual debe ser estimado nuevamente aplicando otra vez la fórmula de evaluación de riesgo y tratando a través de la implementación de más controles. Dentro de los riesgos residuales se debe considerar los que no son de mucha importancia o su prioridad es baja y la organización los acepta. Sobre todo, hay que tomar en cuenta que la estimación del riesgo residual debe ser menor al valor del riesgo identificado la primera vez.

2.6.2. Seleccionando controles apropiados

La opción de tratamiento de riesgo que más se utiliza es la mitigación o modificación del riesgo porque se puede hacer una combinación de seguridad y costo.

Es decisión del equipo de análisis del riesgo identificar los mejores controles para poder tratarlos, pero se puede basar en la ayuda de buenas prácticas para poder establecidos. Por ejemplo, los controles enumerados en el anexo A de la norma ISO 27001. Enumera 114 controles que se dividen en 14 secciones, ya que específicamente nos ayudan a ser una guía para el aseguramiento de información. En resumen, lo que se puede revisar de este Anexo son controles que tiene que ver con:

- *Políticas de seguridad de la información*: cómo se escriben y revisan las políticas.
- *Organización de la seguridad de la información*: la asignación de responsabilidades para tareas específicas.
- *Seguridad de los recursos humanos*: garantizar que los empleados entiendan sus responsabilidades antes del empleo y una vez que han dejado o cambiado de rol.
- *Gestión de activos*: identificación de los activos de información y definición de las responsabilidades de protección adecuadas.
- *Control de acceso*: garantizar que los empleados solo puedan ver información relevante para su rol laboral.
- *Criptografía*: el cifrado y la gestión de claves de información sensible.
- *Seguridad física y ambiental*: asegurar las instalaciones y el equipo de la organización.
- *Seguridad de las operaciones*: garantizar la seguridad de las instalaciones de procesamiento de información.
- *Seguridad de las comunicaciones*: cómo proteger la información en las redes.

- *Adquisición, desarrollo y mantenimiento de sistemas:* garantizar que la seguridad de la información sea una parte central de los sistemas de la organización.
- *Relaciones con los proveedores:* los acuerdos a incluir en los contratos con terceros y cómo medir si dichos acuerdos se mantienen.
- *Gestión de incidentes de seguridad de la información:* cómo informar de interrupciones e infracciones y quién es responsable de ciertas actividades.
- *Aspectos de seguridad de la información de la administración de la continuidad del negocio:* cómo abordar las interrupciones del negocio.
- *Cumplimiento:* cómo identificar las leyes y regulaciones que se aplican a su organización.

Para Implementar estos controles se puede hacer uso de la ISO 27002 que explica cómo se pueden lograr los objetivos de control de la norma.

Si se toma en cuenta aspectos de Ciberseguridad entonces se puede apoyar en algunos controles críticos como base para poder mitigar riesgos que conlleva una organización que está expuesta en el ciberespacio. Para esto tomaremos como referencia los controles críticos establecidos en una guía creada por el Centro de Respuestas ante Incidentes Cibernéticos CERT-PY de Paraguay, realizado en el año 2020 y estos son los que se muestran en la siguiente tabla.

Tabla 22.
Controles críticos

Controles Básicos
Control 1: Inventario de Dispositivos autorizados y no autorizados
Control 2: Inventario de Software autorizados y no autorizados
Control 3: Gestión continua de vulnerabilidades
Control 4: Uso controlado de privilegios administrativos
Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores
Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría

Controles Fundacionales

Control 7: Protección de correo electrónico y navegador web

Control 8: Defensa contra malware

Control 9: Limitación y control de puertos de red, protocolos y servicios

Control 10: Capacidad de recuperación de datos

Control 11: Configuración segura de los equipos de red, tales como cortafuegos, enrutadores y conmutadores

Control 12: Defensa de borde

Control 13: Protección de datos

Control 14: Control de acceso basado en la necesidad de conocer

Control 15: Control de acceso inalámbrico

Control 16: Monitoreo y control de cuentas

Controles Organizacionales

Control 17: Implementar un programa de concienciación y capacitación en seguridad

Control 18: Seguridad del software de aplicación

Control 19: Respuesta y gestión de incidentes

Control 20: Pruebas de penetración y ejercicios de Equipo Rojo

Nota. Tomado de CERT-PY. 2020.

También se pueden considerar controles para vulnerabilidades de aplicaciones Web o móviles basados en lo que recomienda OWASP, etc.

OWASP. - Es un proyecto de código abierto que ayuda a determinar las causas y dar respuesta a vulnerabilidades que hacen el software inseguros, para profundizar el tema puede visitar el sitio: [OWASP Foundation | Open Source Foundation for Application Security](#)

2.7. Monitoreo y reportes del riesgo

Como plantea (Alfaro, 2017) esta etapa consiste en monitorear el comportamiento de los riesgos ante los controles que fueron implementados, medir la eficiencia y eficacia de estos controles como los procesos necesarios para su ejecución.

El monitoreo del riesgo es un proceso sistemático donde se reúne la información necesaria del proceso de gestión de riesgos, verificar si el plan de gestión de riesgos cumplió con los objetivos para el que fue implementado, así como también encontrar problemas y tratar de resolverlos.

Se enfoca tanto en monitorear y mejorar el proceso de gestión de riesgos, como el monitoreo de los factores de riesgo. El equipo de gestión de riesgos debe enfocarse también en identificar nuevas amenazas, así como la reunión de evidencias que apoyen a la toma de decisiones, estar atento a los cambios de escenarios que puedan materializar las amenazas y verificar que si se aplica contramedidas siempre estén alineadas a los criterios de aceptación del riesgo.

Lo que se debe monitorear es:

- Activos
- Amenazas
- Vulnerabilidades
- Nuevas estimaciones de probabilidades e impactos
- Nueva estimación de riesgos encontrados
- Controles establecidos

Con estos puntos monitoreados a la par se verifica que el proceso de gestión de riesgos este correcto y sobre todo siempre esté buscando la mejora continua del aseguramiento y que los objetivos de la gestión del riesgo apoyen los objetivos estratégicos de la organización.

Otro punto importante y que no se debe olvidar es que también debe monitorearse que existan todos los recursos necesarios que apoyen el tratamiento de los riesgos, así como la utilización de herramientas de análisis de vulnerabilidades o de riesgos, que de alguna manera siempre se actualizan.

Una de las herramientas más utilizadas en esta etapa es el uso de indicadores que sobre todo nos den evidencia de que todo está funcionando como se propuso en el plan de tratamiento de riesgo, por ejemplo:

Tabla 23.
Indicadores de monitoreo - Ejemplo

Riesgo/Amenaza	Control	Indicadores
Accesos no autorizados	Autentificación de usuarios a los sistemas utilizando el principio AAA (Autenticación, Autorización y Accounting)	Número de incidentes relacionados con accesos no autorizados

En este ejemplo, cuando se hace el monitoreo lo correcto sería que el número de incidentes se haya disminuido considerablemente, con este ejemplo como base es que se utilizarán estos indicadores para la evaluación de controles implementados.

Desde el punto 2.1 al 2.7 de estudio de esta unidad hemos estudiado todo lo que tiene que ver con el proceso de gestión de riesgos, cabe recalcar que es importante tomar en cuenta que este es un proceso de mejora continua a lo largo del tiempo dentro de una organización y también este proceso de gestión de riesgos es la base fundamental para desarrollar un plan de contingencias o planes de continuidad de negocio, en caso de que alguna amenaza o riesgo se materialice y su impacto paralice los procesos principales de la empresa o afecte a los activos de TI más importantes. El tema de desarrollo de planes de continuidad de negocio se estudiará a profundidad en la unidad 6 de este texto guía.

2.8. Marcos metodológicos para la gestión de riesgos

El proceso de gestión de riesgos se lo puede hacer utilizando metodologías, normas o buenas prácticas que nos ayuden a establecer un proceso ordenado para poder llegar a establecer el tratamiento adecuado de los riesgos. Algunas metodologías son conocidas y desarrolladas con base en normas como las ISO tanto 31000, como la 27005, etc. considerando como el concepto de *riesgo* el punto central de sus procesos.

2.8.1. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT

Creada por el Gobierno español y es de uso público. Está compuesta por una serie de documentos y está totalmente enfocada en el ambiente de tecnologías de información y telecomunicaciones (TIC). Se basa en analizar el *impacto* que puede tener una organización, la violación de la seguridad o el tener expuestos por medio de vulnerabilidades los tres pilares importantes de la organización *Disponibilidad, Integridad y Confidencialidad*, ayudando a identificar las vulnerabilidades por donde se pueden materializar las amenazas y de alguna manera tener una identificación clara de las medidas preventivas y correctivas que se puedan implementar.

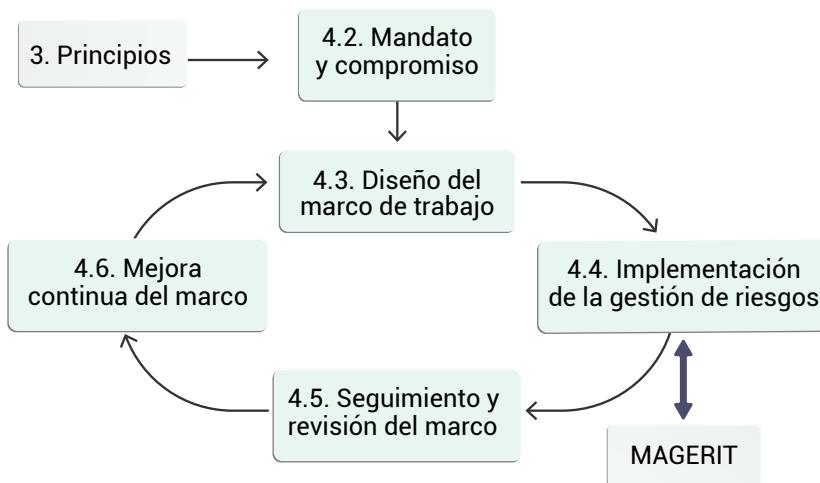
El método de aplicación de esta metodología está basado y orientado a lo que propone ISO 27005 o 31000, de manera que se utilizará incluso la

terminología que propone ISO en cuanto a riesgos. A diferencia de otras metodologías tiene una guía de técnicas que ayudan a dar respuesta a la pregunta ¿cómo hacerlo?

Se integra totalmente a las ISO 27005 y 31000 porque es prácticamente el mismo proceso de gestión de riesgos en ambas normas y con la ISO 27005 MAGERIT tiene una correspondencia directa. En la figura 17 se tiene como se implica MAGERIT en la ISO 27005 o 31000.

Figura 17.

Implicación de MAGERIT en la ISO 27005



Nota. Tomado de MAGERIT, 2016.

En el punto 4.4., Implementación de la gestión de riesgos, en lo que apoya MAGERIT es en un análisis de riesgo más enfocado, más claro y fácil de administrar, porque las ISO darán el qué hacer y MAGERIT apoyará al ¿cómo hacerlo? Pasos de la metodología MAGERIT sugeridas por (Ocampo, 2017):

- Determinar los activos relevantes para la Organización, su interrelación y su valor en el sentido de qué perjuicio (coste) supondría su degradación.
- Determinar a qué amenazas están expuestos aquellos activos.
- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

2.8.2. OCTAVE

Esta metodología está constituida por 4 fases y como toda metodología de análisis de riesgos, siempre busca de alguna manera minimizar los riesgos, las fases de Octave son:

- *Fase 1: Establecimiento de controles por medio de criterios de las métricas de riesgo.*
- *Fase 2: Perfil de Activos por medio del desarrollo de perfil de activos de información y la identificación de los contenedores de estos activos.*
- *Fase 3: Identificación de amenazas mediante la identificación de áreas de preocupación y de los escenarios de amenaza.*
- *Fase 4: Identificación y mitigación de riesgos mediante el análisis de riesgo y selección de formas de mitigación.*

OCTAVE (evaluación operativa de amenazas críticas, activos y vulnerabilidades) son metodologías que funcionan para identificar y evaluar los riesgos de seguridad de la información. Las organizaciones pueden producir protección de información con toma de decisiones de riesgo referidas a CIA (Confidencialidad, Integridad, Autenticación) a los activos de tecnología de información crítica, implementando el método OCTAVE.

OCTAVE se aplica para ayudar a la empresa en términos de:

- Desarrollo de criterios de evaluación de riesgos cualitativos que resulten en la tolerancia al riesgo operacional de la empresa.
- Comprender los activos valiosos para la misión en la empresa.
- Comprender las debilidades y amenazas a los activos.
- Determinación y evaluación de lo que le puede pasar a la empresa si surgen amenazas.

En la figura 18 se puede apreciar cuál es el proceso de esta metodología:

Figura 18.

Proceso de metodología Octave

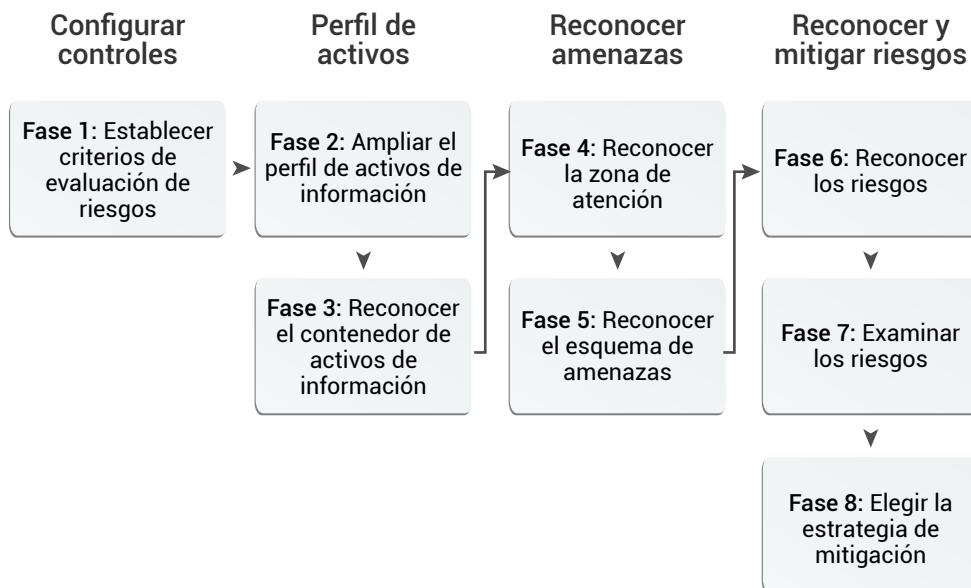


Nota. Adaptado de Las tres fases principales del método principal OCTAVE. (2013). [Ilustración]. https://www.researchgate.net/figure/The-three-main-phases-of-the-main-OCTAVE-RA-method_fig4_308887372

Hay tres métodos de OCTAVE que se pueden aplicar. Estos tres métodos incluyen los métodos OCTAVE, OCTAVE-S y OCTAVE Allegro. OCTAVE Allegro es el que está siendo más utilizado porque se concentró en los activos de información en términos de uso, almacenamiento, transferencia, procesamiento, respuesta a amenazas, vulnerabilidades e interferencias como resultado. Este método tiene 4 fases principales como se puede observar en la figura 19.

Figura 19.

Proceso de metodología Octave Allegro



Nota. Adaptado de Fases y Pasos de OCTAVE Allegro. (2018). [Gráfico]. https://www.researchgate.net/figure/Eight-steps-and-Four-Phases-Octave-Allegro-Method_fig1_327859251

A diferencia de OCTAVE, OCTAVE Allegro se explica en los siguientes pasos como se desarrolla esta metodología según (Ocampo, 2017).

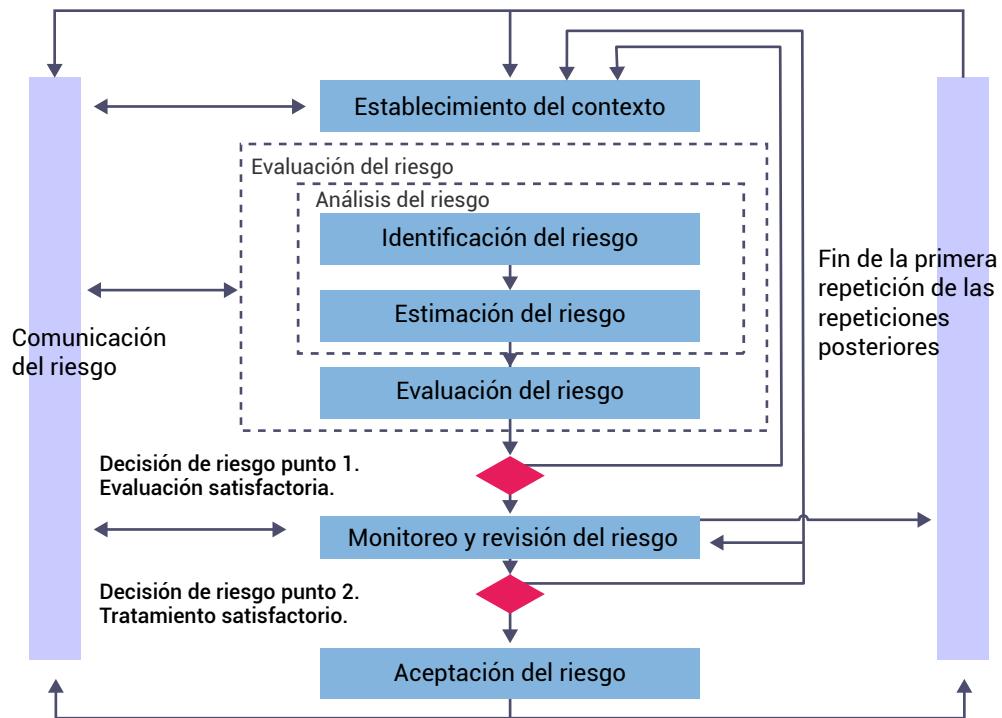
- Establecer criterios de medición del riesgo
- Desarrollar un perfil de activos de información
- Identificar contenedores de activos de información
- Identificar áreas de preocupación
- Identificar escenarios de amenazas
- Identificar riesgos
- Análisis de riesgos
- Seleccionar un enfoque de mitigación

2.8.3. ISO 27005

Pertenece a la familia de las ISO 27000 y está basada en los conceptos específicos de la ISO 27001 y es una guía para ayudar a la implementación de la seguridad de la información basada en el análisis de la gestión de riesgos. Describe un proceso de gestión de riesgos de alto nivel, cuyo objetivo es gestionar los riesgos de algunos activos sobre todo de los que la

organización considera de valor. La figura 20 muestra la estructura de esta norma.

Figura 20.
Estructura ISO 27005



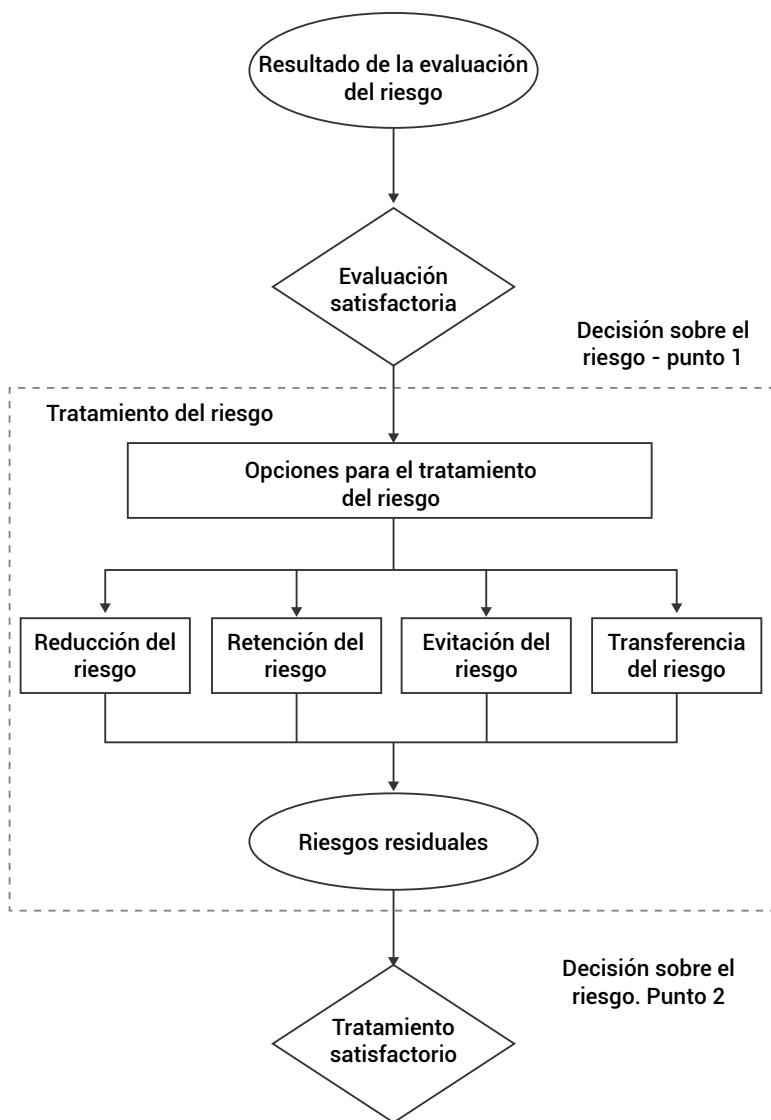
Nota. Tomado de Lozano, M., & Correa, M. (2020). Análisis de las vulnerabilidades de la infraestructura tecnológica mediante testing de caja blanca basada en la ISO 2700.

En el establecimiento de contexto se establece los criterios esenciales para la gestión de la seguridad de la información y se establece el alcance y las restricciones del riesgo que se deben buscar para alcanzar el nivel de seguridad deseado.

En la fase de evaluación del riesgo de seguridad de la información se hace la mediación y descripción del riesgo. Estos resultados ayudarán al equipo de análisis junto con los directivos de la organización a priorizar los riesgos siguiendo la seriedad percibida u otros criterios establecidos. En esta fase se identifica el riesgo, se lo analiza con las probabilidades e impactos y se hace la evaluación que es la estimación del riesgo para priorizar según el resultado de los valores del riesgo y se hace el proceso de tratamiento de estos con base en la actividad descrita en la figura 21.

Figura 21.

Proceso de tratamiento de riesgos ISO 27005



Nota. Tomado de Ocampo, M. (2017). *Revisión de Metodologías de Análisis de Riesgos de la Información*.

Cuando se ha hecho un plan de tratamiento lo que la norma indica es que se establezca la fase de aceptación del riesgo, que es aceptar el plan de tratamiento, aplicar los controles e identificar los riesgos residuales.

Finalmente se recomienda realizar la comunicación del riesgo, desde que empieza el proceso de gestión de riesgos y se lo hace a todos los interesados.

La diferencia principal con la ISO 31000 es que esta norma (ISO 27005) se enfoca a establecer el análisis de los riesgos de los activos de información de la organización con base en el análisis de sensibilidad de estos, esto significa que los criterios a evaluar de estos activos de información son la confidencialidad, integridad y disponibilidad. La ISO 31000 se enfoca en la misma estructura, pero se basa más al estudio de riesgos en general de una organización. Por ejemplo, riesgos ambientales del entorno, de infraestructura, no precisamente buscando el aseguramiento de información.

2.8.4. COBIT 5 for Risk

COBIT 5 for Risk se utiliza como guía en la realización de procesos de gestión de riesgos, ya que define el riesgo de TI como riesgo comercial, es decir, el riesgo asociado con el uso, operación, participación, influencia y adopción de TI dentro de una empresa.

Esta buena práctica considera que el riesgo de TI consiste en eventos relacionados con TI que podrían tener un impacto potencial en el negocio y cuya ocurrencia puede afectar a los objetivos estratégicos del negocio, por lo que hay que considerar que el riesgo de TI siempre existe, sea o no detectado o reconocido por una empresa.

Cobit 5 for Rick maneja los riesgos desde dos perspectivas como lo muestra la figura 22:

Figura 22.
Perspectivas de riesgos según COBIT for Risk



Nota. Adaptado de COBIT 5 for Risk, 2013.

- **Perspectiva de la función de riesgo:** describe lo que se necesita en una organización para construir y mantener actividades de gestión y gobernanza de riesgos centrales, eficientes y efectivas. Para cumplir con esta perspectiva COBIT 5 for Risk define siete principios de riesgo (ver figura 22) que sirven para:
 - Proporcionar un enfoque sistemático, oportuno y estructurado para la gestión de riesgos.
 - Contribuir a resultados consistentes, comparables y confiables.

Los principios de riesgo formalizan y estandarizan la implementación de políticas, tanto la política central de riesgos de TI como las políticas de apoyo. Por ejemplo, política de seguridad de la información y política de continuidad del negocio.

Estas políticas proporcionan una guía más detallada sobre cómo poner en práctica los principios y cómo influirán en la toma de decisiones dentro de una organización.

Figura 23.
Principios para la gestión de riesgos según COBIT for RISK



Nota. Adaptado de COBIT 5 for Risk, 2013.

Para trabajar con los riesgos COBIT 5 for RISK utiliza ciertos procesos de COBIT 5 como se pueden observar en la figura 23.

- Procesos de apoyo clave: rosa oscuro
- Otros procesos de apoyo: rosa claro

Los procesos de riesgo centrales que se muestran en azul claro, también se destacan. Estos procesos respaldan la perspectiva de gestión de riesgos:

- EDM03 Asegurar la optimización de riesgos
- AP012 Gestionar riesgo

Para comprender esta perspectiva de la gestión de riesgos que maneja COBIT, en la guía de esta buena práctica se explica en qué consisten los dos procesos orientados a la gestión de riesgos EDM03 y AP012.

Figura 24.

Procesos para la gestión de riesgos según COBIT for RISK

Figura 33—Procesos principales del riesgo	
Procesos COBIT 5	Razonamiento
EDM03 Asegurar la optimización del riesgo	<p>Este proceso abarca el entendimiento, la articulación y la comunicación del apetito y tolerancia al riesgo de la empresa, y asegura la identificación y gestión del riesgo asociado al valor de la empresa que está relacionado con el uso de TI y su impacto. Las metas de este proceso son:</p> <ul style="list-style-type: none">• Definir y comunicar los umbrales de riesgo y asegurar que se conozcan los riesgos clave relacionados con TI.• Gestionar de una manera efectiva y eficiente a los riesgos críticos de la empresa relacionados con TI.• Asegurar que los riesgos de la empresa relacionados con TI no excedan su apetito de riesgo.
AP012 Gestionar el riesgo	<p>Este proceso abarca la continua identificación, evaluación y reducción del riesgo relacionado con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa. La gestión de riesgos de la empresa relacionado con TI debería ser integrada al ERM global. Se deberían balancear los costos y beneficios de gestionar el riesgo de la empresa relacionado con TI mediante:</p> <ul style="list-style-type: none">• La recolección de datos apropiados asociados al análisis de riesgos.• Manteniendo el perfil de riesgo de la empresa y articulando los riesgos.• Definiendo el portafolio de acciones de la gestión de riesgos y respondiendo al riesgo.

Nota. Adaptado de COBIT 5 for Risk, 2013.

Este marco de referencia se basa también en escenarios de riesgos, es decir, el elemento de información clave necesario para identificar, analizar y responder al riesgo. Los escenarios de riesgo son la representación concreta, tangible y evaluable del riesgo y con esto se pueden utilizar los habilitadores de COBIT 5 para responder a escenarios de riesgo inaceptables.

Hemos finalizado el estudio de contenido planificado para la semana 4. Es necesario que tenga muy claro cómo está estructurada una matriz de riesgo y cómo es el proceso del tratamiento de los riesgos como tal, los estándares o normas más utilizados para la gestión de riesgos. Recuerde apoyarse en bibliografía complementaria disponible digitalmente para que complete su estudio y se recomienda desarrollar las actividades de aprendizaje recomendadas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

Lecturas en bibliografía básica, complementaria y recursos educativos abiertos

- Revise la bibliografía complementaria para afianzar los conocimientos estudiados en la semana 4.
- [¿Cómo crear una Matriz de Riesgos automática?](#)
- **Libro de Gestión del Riesgo de las TI NTC 27005** (Capítulo 7: Evaluación del riesgo. Capítulo 8: Tratamiento y aceptación del riesgo)
- **COBIT 5 for Risk** (Guía de implementación COBIT 5 para Riesgos)

Actividad 1:

Revise los siguientes recursos:

- [OWASP Risk Rating Methodology](#), lea detenidamente cómo funciona esta metodología de análisis de riesgos que es desarrollada por OWASP.
- [Análisis de riesgo aplicando la metodología OWASP](#), lea comprensivamente los conceptos necesarios y cómo funciona la metodología de OWASP.

- Utilice la herramienta [OWASP Risk Rating Calculator](#) con al menos 5 riesgos, donde usted determine cuáles son las probabilidades y el factor de impacto.

Una vez que ha estudiado los conceptos relacionados con la unidad que comprende la semana 3 y la semana 4, le invito a desarrollar la Autoevaluación 2 con el fin de evaluar los conocimientos adquiridos hasta el momento.

¡Éxitos en la autoevaluación!



Autoevaluación 2



Una vez que ha estudiado los conceptos relacionados a la unidad que comprende la semana 3 y la semana 4, le invito a desarrollar la autoevaluación 2 con el fin de evaluar los conocimientos adquiridos hasta el momento.

¡Éxitos en la autoevaluación!

- 1. ¿Cuáles son factores internos que deben considerarse dentro del proceso de evaluación de riesgo?**
 - a. Políticas, procedimientos o normas de la organización.
 - b. Obligaciones legales de la organización.
 - c. A y B son factores internos que hay que considerarlos.
- 2. La probabilidad de que ocurra un riesgo significa:**
 - a. El daño que hace a la organización.
 - b. Cuán factible es que ocurra un evento en el tiempo.
 - c. La amenaza a la organización.
- 3. El impacto cuando se materializa un riesgo significa.**
 - a. El daño que hace a la organización.
 - b. La probabilidad de que ocurra.
 - c. La amenaza a la organización.
- 4. El proceso de identificación de activos es:**
 - a. Identificar las amenazas externas de la organización.
 - b. Identificar los recursos más importantes que quiere salvaguardar la organización.
 - c. Identificar los factores que lo hacen materializarse.

5. Los activos se pueden valorar por:

- a. Probabilidad de amenaza.
- b. Dimensión de impacto.
- c. Por disponibilidad – integridad - confidencialidad.

6. La identificación de vulnerabilidades se refiere a:

- a. Identificar las amenazas externas de la organización.
- b. Identificar los fallos que producen que se materialice la amenaza.
- c. Identificar los factores que lo hacen materializarse.

7. Cuando decimos que las vulnerabilidades pueden encontrarse en aplicaciones, entonces son amenazas a nivel de:

- a. Software.
- b. Hardware.
- c. Personas.

8. Es la actividad de evaluar cuánto afectará a la organización si se materializa una amenaza.

- a. Identificación probabilidad.
- b. Identificación del impacto.
- c. Identificación del riesgo.

9. La matriz de riesgos es una herramienta para:

- a. Evaluar riesgos.
- b. Tratar riesgos.
- c. Mitigar riesgos.

10. Cuando contrata la organización un seguro para que la empresa pueda restablecer sus funciones después de un desastre natural, hablamos de que está:

- a. Mitigando el riesgo.
- b. Aceptando el riesgo.
- c. Transfiriendo el riesgo.

Puede verificar las respuestas de esta autoevaluación al final del texto guía.

[Ir al solucionario](#)

Si su puntaje no es bueno es importante que vuelva a revisar los contenidos de la unidad y los recursos de aprendizaje, no olvide que puede interactuar con su tutor por cualquier medio de comunicación que brinda la UTPL para que aclare sus inquietudes.

Resultado de aprendizaje 6

- Explica los factores clave que intervienen en la autenticación y la forma en que se utilizan para verificar la identidad y permitir el control de accesos a un sistema.

Estimado, para el estudio de la tercera unidad usted debe considerar los diferentes conceptos, definiciones y recursos propuestos, además, debe realizar una verificación de la bibliografía que se cita. Las primeras semanas nos han permitido analizar diferentes conceptos sobre seguridad de la información en estas dos semanas profundizaremos acerca de los ataques a los sistemas. Esto será parte del estudio de la siguiente unidad.

¡Éxitos en el estudio de esta unidad!

Contenidos, recursos y actividades de aprendizaje



Semana 5

Unidad 3. Análisis de ataques a los sistemas de información

En la actualidad el uso de aplicaciones, redes sociales e internet por los temas que son conocidos han aumentado de forma acelerada, muchas actividades que antes se realizaban de forma presencial han pasado a un entorno telemático, como pago de servicios básicos, compras en línea, transferencias electrónicas entre personas naturales por cualquier tipo de negocios, procesos de matriculación en sistemas académicos y así un sin número de operaciones, utilizando casi en la mayoría de transacciones nuestros correos para verificación del proceso es decir nos llegan claves para concluir con la operación, pero ¿Le han solicitado alguna vez cambiar las claves de cuentas de bancos donde usted no tiene cuenta? ¿Le han notificado que su cuenta ha sido suspendida? ¿Le ha llegado un mail con un premio para lo cual debe ingresar a un link o realizar una transferencia bancaria? ¿Lo han tratado de extorsionar por haber ingresado sitios que no lo hizo? Esta es una técnica que los atacantes utilizan conocida como *pishing*, donde se envía mail de forma masiva a la espera de alguna respuesta que le permita obtener cualquier tipo de información, una clave,

una confirmación de que aplicación está utilizando. Muchas de las veces este proceso lo realizan a través de sitios falsos similares los que usted utiliza o confiaría, como por ejemplo www.bancoguayas.com (original), frente www.bancoguays.com (falso); para un usuario final, la falta de cuidado y verificación de una letra faltante y así entrar a un sitio que no es el original puede hacer que se entregue información que el atacante busca.

La seguridad física consiste según (Cristian, 2019) en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al centro y desde el mismo, implementados para proteger el *hardware* y medios de almacenamiento de datos.

El rol principal de la seguridad de los sistemas de información es proteger la información que es manejada por el sistema y además garantizar el adecuado funcionamiento de este. La protección contra intrusos incluye la autorización y restricciones de acceso, así como la ejecución de tareas en entornos seguros, de forma que las actividades relacionadas con los objetivos del negocio sean realizadas íntegramente y sin fallos.

Con estas definiciones podemos comprender que la seguridad informática implica tener en cuenta aspectos físicos, equipamiento tecnológico, sistemas operativos utilizados en los servidores y computadores personales, control de programas maliciosos, el personal que trabaja en la organización, etc. Para tener un sistema de información seguro, todos los aspectos que influyen en dicho sistema deben trabajar de forma sincronizada, evitando problemas que a futuro conlleven al funcionamiento incorrecto del sistema y, por ende, a que la empresa como tal no cumpla sus objetivos de forma adecuada. Un eslabón que falle permitirá que la cadena se rompa.

Los atacantes aprovechan las vulnerabilidades en el software, malas configuraciones en hardware y la falta de compromiso del personal que forma parte del manejo de los sistemas de información para atacar nuestros sistemas. Es importante minimizar el impacto de estos ataques con la utilización de procedimientos y prácticas probadas que facilitan la materialización de actividades delictivas.

Uno de los principales temas a tener en cuenta en seguridad, es la educación; significa entender cuáles son las debilidades más comunes a

ser vulneradas y cuáles son sus riesgos asociados. Esto permitirá conocer de qué manera se realizan los ataques, así como ayudar a identificar otras posibles debilidades, riesgos y desplegar de manera inteligente estrategias de seguridad efectivas.

3.1. Problemas de seguridad de la información

Al hablar de seguridad informática se habla de problemas comunes al momento de implementar un sistema de información, estos van desde aspectos físicos, como la infraestructura a aspectos del manejo lógico de datos, el personal y su interrelación entre estos ámbitos.

Problemas como fallas de hardware (mala configuración de equipos manteniendo las configuraciones del proveedor), fuga de información, ejecutar programas maliciosos, estas fallas son comunes, pero se los puede evitar con una adecuada planificación, compromiso del personal de la empresa y cumplimiento de las políticas de seguridad.

A continuación, se revisará algunos componentes junto con los problemas que estos presentan y que podrían influir en temas de seguridad:

3.1.1. Data Center

Son lugares donde tenemos instalados equipos computacionales destinados a dar servicio a varios terminales. Es necesario ubicarlos en lugares donde no exista humedad o polvo, realizar instalaciones eléctricas adecuadas como la instalación tierra, pararrayos, utilizar equipos que permitan regular el voltaje o equipos estabilizadores de voltaje como UPS, etc., con todo esto se evita que los equipos de cómputo sufran averías, lo que podría conllevar a pérdida de información. La pérdida de información puede determinar la desaparición de una empresa, puesto que la información se considera como el activo más valioso y recuperar en algunos casos es imposible. Con las complicaciones que se puede tener, también podría ocasionar que la empresa tenga pérdidas económicas muy cuantiosas, llegar a un incumplimiento con los clientes, la reputación de esta ante la competencia.

Las salas de servidores deben ser lugares donde solamente pueda acceder personal autorizado, con medidas de seguridad necesarias como puertas de emergencias, extintores, etc., debe cumplir con estándares mínimos de

seguridad, así como creación de políticas para el acceso. Su ubicación debe ser en un lugar donde solo tengan acceso físico las personas encargadas, debe estar en un sitio donde se pueda monitorear la entrada y salida de las personas y su puerta de acceso debe estar a la vista de los directivos o de los encargados.

Realicemos una síntesis. Trataremos de poner en consideración algunos aspectos que es necesario mantener como medidas de seguridad nuestro DataCenter:

- Combinar la seguridad física y lógica.
- Verificar la correcta instalación eléctrica, contando con equipos que permitan realizar tareas esenciales ante la falta de energía eléctrica.
- Mantener un cableado estructurado de red.
- Ubicación adecuada para poder controlar el acceso.
- Políticas de control de acceso y manipulación de los servidores.
- Bitácoras de acceso en el caso de realizarlo de forma automática.
- Definir niveles de autorización del personal que accede, ya sea físico como remoto las 24 horas.
- Si es posible se debe implementar sistemas de video vigilancia con activación.
- Poseer un sistema rápido de reportes de acceso a la sala.
- Mantener un sistema adecuado para poder mitigar los riesgos.

Figura 25.

Control de acceso mediante dispositivos (clave de acceso, tarjeta, control biométrico)



Nota. Tomado de (PNGEGG, n.d.)

3.1.2. Servidores

Un servidor es un computador, el cual posee un gran poder de procesamiento, son utilizados en algún servicio específico, como almacenar gran cantidad de información a través de una base de datos, realizar el servicio de impresión, almacenar y compartir archivos entre diferentes usuarios, se debe señalar aquí que los sistemas operativos pueden ser diferentes siendo esto muchas veces transparente a los usuarios finales. En una empresa u organización un daño sobre este tipo de recursos puede ser crítico, siempre y cuando no se cuente con unas políticas adecuadas de almacenamiento y respaldo de la información, lo que conllevaría a perder la información valiosa para la empresa, que es el activo más importante.

En este tema se debe considerar:

- Respaldos en dispositivos externos, si es posible los mismos deben estar en otro sitio, en la actualidad se pueden utilizar servicios en la nube.
- No utilización de servidores en tareas cotidianas como utilización de navegadores, colocar memorias para copias, descarga de archivos por tener conexiones más rápidas.
- Políticas de respaldos y responsables de los procesos.
- Uso centralizado de mantenimiento de claves, ante riesgos de problemas con los administradores de los servidores.
- Activar las auditorias de acceso para poder obtener reportes de acceso, uso de aplicaciones y manipulación del hardware del servidor.

En la actualidad este servicio se está traslado hacia terceros, es decir, los equipos necesarios como tal, están en empresas proveedoras de este tipo de recursos como por ejemplo, una empresa puede contratar un servidor con un número de procesadores, memoria RAM específica, espacio de almacenamiento. En la figura 26 se puede observar una colección de servidores dentro de un data center.

Figura 26.

Servidores dentro de un data center



Nota. Tomado de Andalucía (2021).

Señalar en este tema que una buena parte de los problemas relacionados con la seguridad está controlada por el proveedor. La nube entonces son los entornos de hardware y software donde se ejecutarán las aplicaciones. Estas aplicaciones serán accesibles desde cualquier dispositivo que se encuentre conectado a la red.

Además, debemos dejar claro que en la actualidad las empresas están orientando el trabajo hacia la nube (CLOUD), estos servicios se ejecutan a través de Internet. Es aquí donde cada día los problemas de seguridad van aumentando por la cantidad de vulnerabilidad que cada día aumentan entonces el control que se debe tener sobre los servidores de cada empresa es mayor.

3.1.3. Puertos

Son canales de comunicación que nos permiten el acceso a un servicio. Por temas de seguridad en un servidor es necesario tener habilitados únicamente aquellos puertos que son estrictamente necesarios para brindar el servicio para el que ha sido encomendado dicho equipo, esto no solo por optimización de recursos (memoria, procesador, etc.) sino también como se ha mencionado por seguridad. El tener puertos sin control o abiertos, implica que por dichos puntos de acceso pueden ser entradas para realizar un ataque o explotar una vulneración del sistema.

Ocasionalmente se abre puertos con el fin de hacer pruebas o por error, por lo cual es necesario el periódico escaneo de puertos abiertos, con el fin de cerrar aquellos que no se estén utilizando. Otra forma de evitar tráfico por puertos no deseados es mediante listas de control de acceso, que permitan sólo el tráfico necesario. Las listas de control de acceso deben ser creadas de acuerdo con las necesidades de la empresa y no solo se debe controlar el tráfico entrante, sino también el tráfico saliente.

Existen herramientas gratuitas las cuales son muy fáciles de utilizar como el [NMAP](#) y que permiten realizar un escaneo de un equipo (servidor o máquina personal) determinando que puertos están abiertos, por lo general al hacer este escaneo se podrá visualizar el puerto identificado con su número, el servicio que está realizando y además que usuarios están conectados y algunas otras funcionalidades, esta es una aplicación de código abierto. En KaliLinux podemos ejecutar el siguiente comando:

```
sudo nmap -a // nos permitirá determinar los puertos que se encuentran utilizando
```

En este recurso video de YouTube: [Cómo descargar e instalar NMAP uso básico](#)), podrá hacer un inicio con la herramienta.

Para reforzar este tema le recomiendo realizar la *Actividad 1* en las actividades recomendadas al final de esta semana.

Un sistema está constituido esencialmente por el elemento fundamental que es la información. Un *sistema de información* tiene como principal objetivo gestionar los datos para almacenarlos como información que posteriormente apoyen los procesos de negocio de la empresa. En el siguiente apartado revisaremos los conceptos más a profundidad.

3.2. Software en la organización

El *software* como parte fundamental en la organización ha permitido agilizar los procesos del negocio dentro de la organización. Podemos encontrar entonces que las organizaciones cada vez están implementando software de diferente tipo, como: sistemas operativos, aplicaciones de ofimática, software a la medida para un problema específico de la organización, servicios de mensajería internos, comunicaciones, administración de

hardware, sistemas transaccionales, aplicaciones móviles, etc. Además, han influido muchos factores adicionales para estas nuevas implementaciones como:

- Crecimiento de las transacciones de la organización.
- Crecimiento de personal que trabaja en la empresa.
- Nuevas necesidades de los clientes.
- Mayor competitividad por las empresas del entorno.
- Uso de nuevas tecnologías.
- Mayores demandas de servicios.
- Cambios en políticas que influyen en la organización.

Todos estos cambios deben ser considerados por los gobiernos de TI para mantener la continuidad del negocio. Esto significa que los problemas que se presenten relacionados con temas de seguridad deben ser considerados permitiendo mantener la reputación de la empresa.

En el caso del software a la medida, esto se ha realizado mediante la implementación de software desarrollado dentro de la organización o con la adquisición a proveedores de estos servicios. Dejemos por el momento la arquitectura que se utilizará para su implementación. En muchos de los casos las organizaciones conforman internamente sus grupos de desarrollo de sistemas con la finalidad de realizar un software para una necesidad de la organización o en ocasiones también para integrar nuevas funcionalidades sobre sistemas ya existentes.

Otra forma es la implementación de un software adquirido a un proveedor que ya tienen una solución a medida de la organización, ayudada por factores como: estabilidad, funcionalidad, tiempo de implementación contra un desarrollo interno, etc. etc. A través de los tiempos las tecnologías que han surgido para almacenar y acceder a este sistema han crecido en forma acelerada por la cantidad de información, las necesidades de acceso que sobre el sistema necesitan las organizaciones, la ubicación de sus usuarios, costos de almacenamiento, etc.

Es así como han surgido varias formas de contar con sistemas dentro de las organizaciones, entre otras podemos considerar:

- *In house*, los equipos están en la organización y los sistemas han sido desarrollados *in situ*, por lo que se ha de invertir en la actualización del hardware, esto ayudará a mantener un control de los sistemas, sus actualizaciones, sus datos. El acceso remoto a la información será una preocupación dentro de la organización.
- *As service*, la empresa no se ha de preocupar por las actualizaciones del hardware pues estos serán administrados por terceros. Los sistemas pueden ser un servicio donde la empresa no se ha de preocupar por los cambios o como un *hosting* donde la organización actualizará el software. En estos casos la organización no administra la información que se producen en los sistemas.
- *In house as service*, la infraestructura del hardware de la organización será de su competencia, pero los SI y actualizaciones de estos pertenecerán a proveedores. En este caso la organización garantiza tener la información de forma interna.

3.3. Seguridad del software

El proceso de desarrollo de software debe contemplar desde sus etapas iniciales, las empresas que desarrollan tardan en considerar los requisitos de seguridad, no son considerados en la etapa delicitación de requisitos del sistema, sino más bien en etapas de implementación.

Deben entonces considerarse aspectos relacionados según explica en López Álvarez, 2020 como:

- Requerimientos de seguridad y casos de abuso
- Análisis de riesgos
- Pruebas basadas en riesgos de seguridad
- Revisión de código con uso de herramientas
- Pruebas de penetración

El detalle de estos temas se tratará a profundidad en el apartado 4.1. Importancia del desarrollo seguro.

3.4. Ataques a los sistemas de información a través de Internet

La seguridad del software debe enfocarse al proceso de desarrollo de aplicaciones, con la aplicación de políticas claras que permitan estandarización de procesos desde la etapa de planificación hasta la implementación. Durante el proceso de desarrollo del sistema de información, se debe considerar los problemas que puedan afectarlo una vez que entre en funcionamiento.

Como se ha mencionado la evolución de la tecnología y sus procesos de interacción, da paso también al surgimiento de nuevas modalidades delictivas y formas de ataques. Por ejemplo, hace muy poco tiempo el uso de aplicaciones bancarias en línea era muy limitado, en la actualidad es casi una práctica común entre las personas, es así que los usuarios sin los debidos procedimientos pueden considerar al Internet y las tecnologías informáticas como aspectos negativos que influirán también en la empresa.

A diario se descubren nuevas vulnerabilidades en los sistemas de información y los responsables de TI deben en su totalidad comprender la importancia que tiene la seguridad y cómo abordar este grave problema desde diferentes puntos de vista.

Así que debemos tener claro que casi la totalidad de ataques se dan vía internet o que es necesario estar conectados a una red de comunicación. Se consideran cinco fases por las cuales suele pasar un ataque cuando es ejecutado, de esta manera para poder dar respuesta a un ataque debemos conocer cómo se realiza el mismo, este es un tema que se aborda en *hacking ético*.

De esta manera las fases por las que un ataque suele pasar son descritas en el siguiente recurso:

Fases de un ataque informático

Cree usted que alguno de los sistemas donde ha registrado sus datos ha sido hackeado ¿Alguien conoce una clave que usted utilizó? ¿Cómo saberlo? Lo invito a realizar la Actividad 2 al final de esta semana para reforzar sus conocimientos.

Para reforzar este tema en el segundo bimestre en el apartado 5.7 manejo de incidentes informáticos se realiza una explicación en cuanto a análisis forense, cómo actuar ante un incidente informático.

3.5. Tendencias de los ataques

Existen algunos motivos significativos que debemos considerar han propiciado un ambiente cada vez más accesible para la realización de ataques a las organizaciones, como:

- El incremento de dependencia a las TIC por parte de la sociedad actual, permitiendo un aumento potencial de los daños que se pueden producir tanto a las empresas como a los clientes.
- La cada vez mayor accesibilidad y familiaridad con las TIC aumenta el nivel de amenazas.
- Los constantes cambios morales en la sociedad crean personas dispuestas a causar daños por diferentes razones como económicas, psicológicas, terroristas o simplemente por un ego personal.
- Aunque en algunos países existen estrictos controles legislativos respecto a brechas de seguridad en la información, no en todos los países estos se aplican con la misma rigidez lo que permite cierta flexibilidad al atacante.
- El desarrollo de nuevas herramientas para aumentar la vulnerabilidad.



Hemos terminado con el estudio de la presente semana. ¿Cómo le fue con los contenidos? Recuerde que si es necesario profundizar en algún tema puede contactarse por los medios conocidos con el profesor tutor.



Actividades de aprendizaje recomendadas

Es hora de realizar la práctica de algunos de los temas tratados, para lo cual le sugiero realizar las siguientes actividades:

- Revise el siguiente video mirar el siguiente video: [Qué son los PUERTOS de un Servidor](#) para una mejor comprensión de tema sobre el manejo de puertos
- Revise el video [IP Servicios Puertos Protocolos](#) para reforzar los contenidos del tema.

▪ Actividad 1:

Búsqueda de puertos en el sistema.

Estimado estudiante, para reforzar sus conocimientos, investigue cuáles son los principales puertos de entrada/salida dentro de los sistemas y periféricos.

Por ejemplo, MySQL utiliza el puerto 3306 por defecto para la conexión, con esta base de datos es muy común tener un inconveniente con la aplicación Skype que utilizan el mismo puerto.

Figura 27.

XAMPP

The screenshot shows the XAMPP Control Panel interface. At the top, it displays 'XAMPP Control Panel v3.2.1 [Compiled: May 7th 2013]'. Below this is a table with the following data:

Module	Service	Module	PID(s)	Port(s)	Actions
		Apache			<button>Start</button>
		MySQL	10568	3306	<button>Stop</button>
		FileZilla			<button>Start</button>
		Mercury			<button>Start</button>
		Tomcat			<button>Start</button>

Así mismo, muchas aplicaciones en sus url dejan de forma explícita el puerto que están utilizando <http://190.214.14.228:8081/> el mismo que puede brindar información a los atacantes.

A partir de esta información podría realizar lo siguiente:

1. Abrir una consola del sistema (Windows) como administrador.
2. Ejecutar el comando:

netstat -ao esto permitirá ver los puertos que están trabajando actualmente

Proto	Dirección local	Dirección remota	Estado	PID
TCP	0.0.0.0:135	CITTE-CCCEL-025:0	LISTENING	1272
TCP	0.0.0.0:445	CITTE-CCCEL-025:0	LISTENING	4
TCP	0.0.0.0:5040	CITTE-CCCEL-025:0	LISTENING	5236
TCP	0.0.0.0:7070	CITTE-CCCEL-025:0	LISTENING	3180
TCP	0.0.0.0:21112	CITTE-CCCEL-025:0	LISTENING	4
TCP	0.0.0.0:49664	CITTE-CCCEL-025:0	LISTENING	68
TCP	0.0.0.0:49665	CITTE-CCCEL-025:0	LISTENING	968
TCP	0.0.0.0:49666	CITTE-CCCEL-025:0	LISTENING	2000
TCP	0.0.0.0:49667	CITTE-CCCEL-025:0	LISTENING	2128
TCP	0.0.0.0:49668	CITTE-CCCEL-025:0	LISTENING	3776
TCP	0.0.0.0:49669	CITTE-CCCEL-025:0	LISTENING	68
TCP	0.0.0.0:49679	CITTE-CCCEL-025:0	LISTENING	1008
TCP	127.0.0.1:50911	CITTE-CCCEL-025:0	LISTENING	4168
TCP	127.0.0.1:50912	CITTE-CCCEL-025:0	LISTENING	4284
TCP	192.168.16.7:139	CITTE-CCCEL-025:0	LISTENING	4
TCP	192.168.16.7:49692	relay-98c2795c:http	ESTABLISHED	3180
TCP	192.168.16.7:49711	52.177.165.30:https	ESTABLISHED	4316
TCP	192.168.16.7:49801	a23-54-148-225:https	CLOSE_WAIT	7300
TCP	192.168.16.7:49804	a23-54-148-225:https	CLOSE_WAIT	7300
TCP	192.168.16.7:50039	a23-54-149-137:https	CLOSE_WAIT	4128
TCP	192.168.16.7:50987	a23-54-149-137:https	CLOSE_WAIT	4128
TCP	192.168.16.7:50988	a23-54-149-137:https	CLOSE_WAIT	4128

3. Si desea buscar como está un determinado puerto podría utilizar:

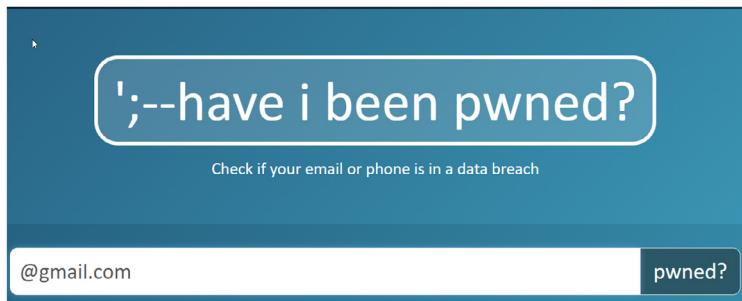
netstat -ao | find 8080 nos permitirá ver cómo están las conexiones por ese puerto.

Aquí puede encontrar información del tráfico que se está realizando sobre el computador, qué puerto está siendo ocupado y el estado.

- **Actividad 2:**

Búsqueda de información para detectar si un correo utilizado en un sistema que ha sido hackeado, esto le podrá ayudar con los colaboradores de su organización o empresa para determinar si los correos utilizados en alguna aplicación que ha sido hackeada deberían entonces actualizar sus contraseñas.

Ingrese al sitio [have i been pwned/](http://haveibeenpwned.com)



En el mismo sitio también podrá encontrar un link donde puede revisar si un determinado [password](#) ha sido encontrado en alguna base de datos hackeada

A screenshot of the "Pwned Passwords" section of the Have I Been Pwned? website. The section title is "Pwned Passwords". Below it is a paragraph of text explaining that pwned passwords are 613,584,246 real world passwords previously exposed in data breaches. It states that these passwords are unsuitable for ongoing use due to increased risk of being used to take over other accounts. They are searchable online and downloadable for use in other systems. A link to "Read more about how HIBP protects the privacy of searched passwords." is provided. At the bottom is a search bar with the word "password" and a "pwned?" button.

Otro sitio Web que tiene una funcionalidad similar es [AVAST](#) :

A screenshot of the Avast Hack Check website. The main title is "Did your password leak online?". Below it is a subtitle "Find out with Avast Hack Check". A text box explains that users just need to enter their email and the site will check if any accounts linked to it have been compromised. There is a text input field for "Enter your email address" and a green "CHECK NOW" button.

Como le fue con este tema, ha podido encontrar alguna información que le ha sido útil y que ha podido ayudar para determinar si su correo está dentro de algún sitio que ha sido hackeado.

En esta semana continuaremos con este tema interesante como es el análisis de ataques a los sistemas de información, además consideraremos otras alternativas que pueden ayudar a un atacante como es la utilización de las personas pues no únicamente los ataques se llevan a cabo por problemas de vulnerabilidades en el software.



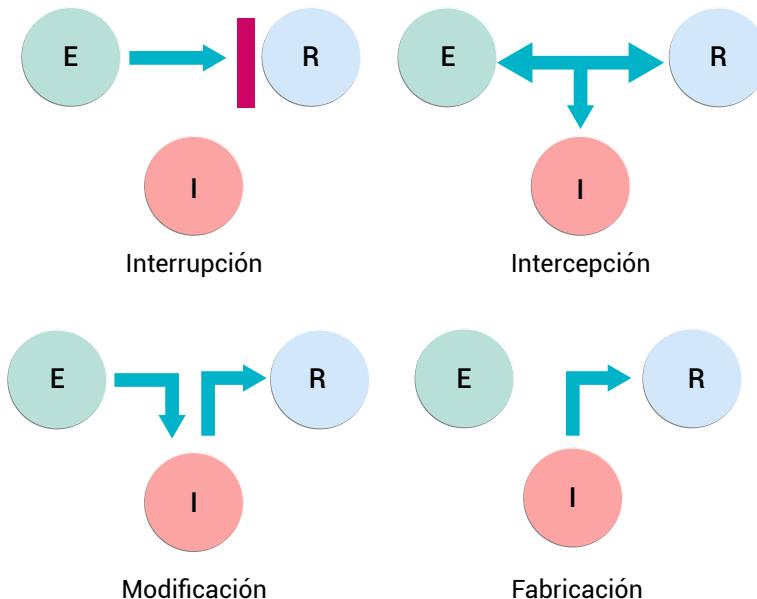
Semana 6 y 7

3.6. Ataques a los sistemas

Para mitigar eficazmente el impacto provocado por ataques a los sistemas, es de vital importancia conocer de qué manera se realizan y cuáles son los puntos vulnerables para explotar sobre los cuales se enfocarán los esfuerzos tendientes a su prevención.

Un ataque no es más que la materialización de una amenaza. Así, en la figura 28, se categorizan cuatro tipos generales de amenazas o ataques.

Figura 28.
Tipos de ataque de sistemas de información



Nota. Tomado de ISACA, 2013.

- **Interrupción:** este es un ataque contra la *disponibilidad*, en el cual un recurso del sistema puede ser destruido o volverse no disponible. Por ejemplo, la destrucción de elementos de hardware, corte de líneas de comunicación o des habilitación de sistemas.
- **Intercepción:** en este ataque contra la *confidencialidad*, una entidad no autorizada como una persona, un programa o un computador consigue acceso a un recurso. Entre los ataques de este tipo podemos tener: interceptar una línea de transmisión para copiar datos que circulen por la red, copia ilícita de ficheros o programas (intercepción de datos) o bien la lectura de las cabeceras de paquetes para develar la identidad de uno o más de los usuarios implicados en la comunicación observada ilegalmente (intercepción de identidad).
- **Modificación:** este es un ataque contra la *integridad* en el cual además de acceder a un recurso, se realiza manipulación de su información. Entre los ejemplos de este tipo de ataque podemos mencionar: cambio de valores en un archivo de datos, alteración de un programa para que funcione de diferente forma y además se puede modificar el contenido de mensajes que están siendo transferidos por la red.
- **Fabricación:** este es un ataque contra la *autenticidad* caracterizada por la inserción de objetos falsos en el sistema. Estos ataques pueden así mismo clasificarse como pasivos y activos.
 - **Pasivos.** No se altera la comunicación, únicamente es escuchada o monitorizada, para obtener la información al ser transmitida. Tiene como objetivos la intercepción de datos y análisis de tráfico. Los ataques pasivos son difíciles de detectar, ya que no provocan ninguna alteración de los datos.
 - **Activos.** Implican la modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Entre los tipos de ataques activos tenemos:
 - *Suplantación de identidad*, en la que se puede usar secuencias de autenticación capturadas y repetidas.
 - *Reactuación*, en donde los mensajes legítimos son capturados y repetidos para producir un efecto indeseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

- *Modificación de mensajes*, en donde una porción del mensaje legítimo es alterada, o retardados o reordenados, para producir un efecto no autorizado.
- *Degradación fraudulenta* del servicio que impide el uso normal o la gestión de recursos informáticos y de comunicaciones.

Se realizará una especificación de acuerdo hacia donde los ataques están destinados, así:

3.6.1. Ataques destinados a páginas y portales Web

Los sitios Web, dado su carácter público son un foco perfecto para los atacantes, los cuales, basados en sus aspectos técnicos, determinan la forma en que pueden obtener el control parcial o total de este y utilizarlo para sus propósitos. A continuación, se nombra brevemente los principales tipos de ataques que pueden utilizarse para tal fin, de entre los cuales se escogerán los más relevantes para ampliar su descripción:



Para reforzar este tema le recomiendo realizar la *Actividad 1* en las actividades recomendadas al final de esta semana

Existen muchas herramientas que, aunque no se debería promulgar su uso, deben considerarles desde otro punto de vista, es decir, que nos ayudan a escanear sitios Web y determinar si el mismo es vulnerable o no. Estas herramientas pueden servir también al personal de TI para que realicen procesos internos y poder determinar si nuestros propios sitios cuentan con vulnerabilidades. Como se ha dicho, nunca se debe decir a nosotros no nos pasará o nuestro sitio está asegurado. Debemos siempre mantenernos a la defensiva. Uno de los sitios es punkSpider.org, por lo que lo invito a que entre al mismo y se familiarice con sus funcionalidades.

3.6.2. Ataques destinados a personas y usuarios de Internet

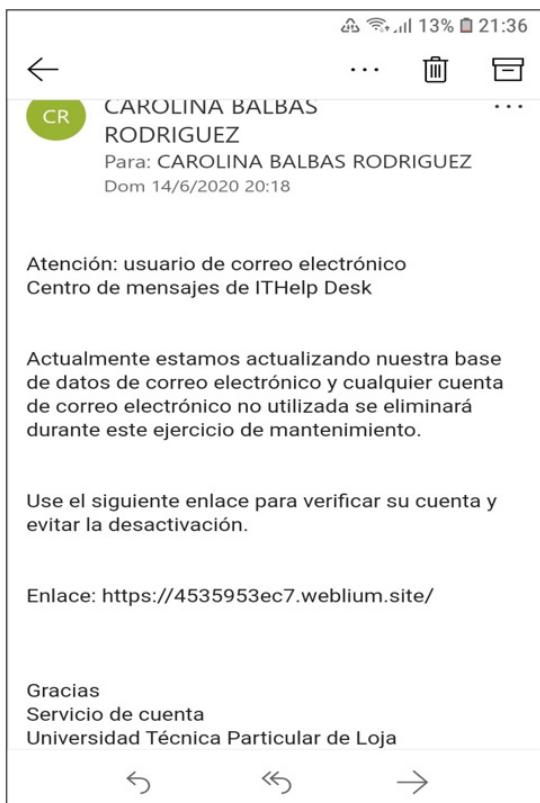
En la actualidad la mayoría de usuario que se encuentren conectados a Internet estará expuesto a problemas de seguridad y depende de cada uno el estar protegido y atento a este tipo de problemas. Vamos a continuación, a nombrar algunos de los principales tipos de ataques que suelen utilizarse. Existen un sin número de estos, pero trataremos de hablar de los más relevantes ampliando su descripción:

Phishing: utilizando diferentes métodos se intenta obtener datos personales de las posibles víctimas, el más conocido es la suplantación de páginas Web, mediante la creación de un sitio similar a otro sitio original con el fin de que el visitante ingrese y deje sus datos personales como claves, números de tarjeta etc. Por lo general este tipo de ataques se dan por medio del correo electrónico, suplantando empresas y entidades financieras y logrando así hacernos ingresar a sitios Web falsos.

Algunos de los correos, pese al control que está configurado en los servidores de correo, pasan directamente a la bandeja de entrada.

Figura 29.

Correo tipo spam



Como se puede ver en la figura 29 el enlace a donde se pide dirigirse no tiene nada relación con el sitio en este caso de la universidad, por lo que si los usuarios reportan dicho correo se puede realizar algunas acciones:

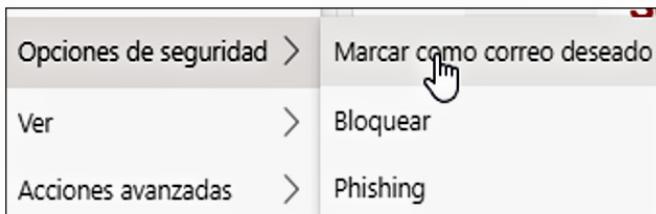
- Revisar el código fuente del correo donde podemos encontrar información desde el servidor desde donde se está enviando el mail.
- Si se está enmascarando el mail original, es decir, cambian el nombre de quien lo envía USUARIOXYUTPL, pero al momento de revisar el código nos damos cuenta de que el mail que se utiliza es **pxyszss@xyz.com** que no tiene relación con un correo institucional.
- Nos podemos ayudar también pasando el ratón sobre el enlace de un correo, se revelará el URL vinculado original antes de abrirlo.

Se debe considerar este tema ya que muchas de las veces los usuarios entregan sus claves ante amenazas para una rápida respuesta. Es así como la implementación de mecanismos de seguridad en los sistemas ayudará a elevar el nivel de seguridad en los mismos.

El *pishing* se puede combatir al interno de las organizaciones, concientizando a los usuarios a no abrir correos que no tengan seguridad de quien los envía y ayuden a reportarlos como correo no deseado con procesos muy fáciles que ya muchos de los clientes de correo ya los tienen. En la figura 30 se muestra como en el cliente de Outlook de office 365 se puede realizar esta tarea.

Figura 30.

Proceso para reportar un correo como spam en Outlook



Vishing, es realizado mediante llamadas telefónicas a las personas. Se trata de extraer cualquier tipo de información que pueda servir para un posterior ataque. Por ejemplo ¿le llamamos del banco tal? La persona dice no tengo cuenta en el banco. Posterior a eso se hace una nueva llamada ahora desde otro banco hasta saber en dónde tiene una cuenta.

Smishing, utiliza un mensaje de texto SMS para solicitar un código o el ingreso a un link para realizar una determinada acción, debemos aquí nuevamente señalar que el proceso de concientización y capacitación a

los empleados ayuda mucho. Generalmente consideramos que esto no afectará a la empresa, pero si un atacante se hace de una cuenta de correo empresarial el envío de mensaje a los otros empleados será más creíble la información que se solicite o se ejecute un archivo que permita instalar por ejemplo un *malware* en la red cooperativa.

Spoofing: consiste en suplantar la identidad del computador de una persona, mediante la sustitución de datos. Se realiza cuando se crea una conexión entre dos máquinas y una tercera ingresa en medio de la comunicación, suplantando la identidad de la otra utilizando, podemos encontrar varios tipos:

- Suplantación de dirección IP, esto le puede permitir vulnerar la protección de un *firewall*.
- Email *spoofing*, utilizará la dirección de correo de una entidad confiable
- Suplantación de DNS, permite acceder a los servidores de nombres de dominio de la víctima para modificar sus direcciones IP redirigiendo a servidores maliciosos.

Podemos señalar como la forma más usada en este tipo de ataque la suplantación de correo electrónico, esto con el fin de poder obtener claves de acceso en un proceso de recuperación, códigos para la ejecución de transacciones bancarias que utilizan doble factor de identificación, pedir información sobre clientes/transacciones reportes financieros a empleados haciéndose pasar como el gerente, etc. Para esto se debe informar este tipo de ataques a todos los empleados para que cuando se presente algo inusual este sea validado por otro medio.

Scam: cuando se ofrece regalar dinero a cambio de más dinero. El atacante ofrece extrañas recompensas, herencias de dudoso origen o premios de otros países, los cuales para ser reclamados piden una suma de dinero inferior a la que se recibirá a cambio. Normalmente eso hace referencia al llamado fraude nigeriano, ya que muchas de las direcciones que se utilizan para el envío de mail están ubicadas desde ese país. En la figura 31 se muestra un ejemplo, donde se ofrece una jugosa cantidad de dinero, pero luego de hacer todo el seguimiento se debe primero realizar una transferencia para poder habilitar la *dichosa cuenta*.

Todos estos ataques de ingeniería social deben ser socializados con el personal de la organización desde el departamento de TI como

responsables de la seguridad, pues muchas veces además de estas ofertas puede llevar a la entrega de datos y claves personales, o de alguno de los sistemas que se manejan.

Figura 31.

Correo tipo Scam (conocido también fraude nigeriano)

Querido en el señor,

① Este mensaje ha sido identificado como un correo no deseado. Se eliminará después de 30 días
② Etiqueta: Junk Email (30 días); fecha de vencimiento: Vie 3/9/2021 11:30

MO ecowasfundstop1@gmail.com en nombre de
Marina Oswald <mr4help@gmail.com>
Mié 4/8/2021 11:30

Querido en el señor,

Con el debido respeto y humanidad, permítanme en primer lugar informarles, obtuve su dirección de correo electrónico de un directorio de correo y decidí enviarle un correo para obtener un permiso para seguir adelante.

Soy la señora Marina Oswald de Suiza. Estoy casada con el señor Tom Oswald, quien trabajó con una empresa de construcción en Asia durante veinte años antes de morir en los desastres del tsunami, estábamos casados pero sin hijos.

Desde su muerte decidí no volver a casarme. Deposité la suma de cuatro millones quinientos mil dólares estadounidenses (\$ 4.5 millones) en el banco. Y ahora estoy dispuesto a donar esta suma de \$ 4.5 millones a los menos privilegiados y contribuir al desarrollo de la iglesia en África, América, Asia y Europeo.

Ingeniería social: el atacante busca suplantar personas y entidades para obtener datos personales; estos ataques se suelen realizar mediante llamadas telefónicas, mensajes de texto o falsos funcionarios. Su objetivo es el de obtener datos importantes para después manipularlos, analizarlos y utilizarlos en contra de la víctima. Aquí podemos encontrar el sexting como una estafa sexual hacia las personas, esto se da por la llegada de un archivo fotográfica a una víctima por ejemplo por Whatsapp al momento de revisarla el atacante se informa de esa lectura y luego utiliza esta información para adentrar y pedir ya sea fotos sexuales de la víctima o extorsionar con dinero asustando que es pornografía infantil y que lo denunciará ante la policía y al avisar su teléfono se podrá ver que la persona si tiene la foto. Si es uno de nuestros empleados posiblemente pedirá información de la empresa pues los atacantes conocer el nivel jerárquico de la organización. Es por eso que la continua capacitación es fundamental, así como la configuración

de los equipos y aplicaciones, ejemplo no abrir archivos de contactos no registrados.

¿Cómo protegerse?

Recuerde que la capacitación y la divulgación entre empleados de la empresa es una buena de protegerse contra las técnicas de ingeniería social. Mucha de estas técnicas se puede prever utilizando el sentido común y no divulgando información que podría poner en peligro la seguridad de la empresa. Sin importar el tipo de información solicitada, se aconseja que:

- Averigüe la identidad de la otra persona que solicita información solicitando (apellido, nombre, compañía, número telefónico),
- Antes de abrir cualquier archivo, verifique si realmente la información corresponde a usted,
- Pregúntese tan importante es la información que nos solicitan.

En este contexto, puede ser necesario capacitar a los usuarios para que tomen conciencia acerca de los problemas de seguridad

OSINT

OSINT (Open Source Intelligence) se puede catalogar como el conjunto de técnicas y herramientas para recopilar información pública, analizar los datos y para convertirlos en información relevante. Las personas al utilizar Internet en sus diferentes aplicaciones y redes sociales almacén información sobre lugares que han visitado, personas con las que han estado, sus gustos por la política, deportes y muchas cosas más, las personas no están conscientes que la información está expuesta públicamente y puede ser utilizada por cualquier persona, con diferentes objetivos. A veces se dice ¿Cómo es posible que justamente nos roben el fin de semana que salimos de vacaciones? Si cuando estamos empacando ya subimos las fotos a nuestras redes *saliendo de vacaciones con toda la familia*.

Según (Pastorino, 2019) OSINT al igual que otras metodologías se tiene diferentes fases: Planificación, selección de fuentes, obtención de datos, procesamiento, análisis y reporte. Cada una de estas fases son importante para poder tener datos claros y poder obtener la información que es necesaria de lo contrario podemos confundirnos ante la gran cantidad de información que nos llegue. Igualmente, para iniciar con esta metodología

se recomienda las [Guías de Flujos de Trabajo de Ciberpatrulla](#), que lo invito a que la revise, pues permite familiarizarse con el proceso.

Algunas herramientas de OSINT

(Pastorino, 2019) nos presenta algunas herramientas. Vamos a mencionar algunas de estas. En cada una están los *links* de las mismas que puede usted realizar:

- [Geo Social Footprint](#), pueden ser utilizadas para realizar búsquedas de noticias o posteos en una determinada ubicación.
- En el sitio [Newspaper Map](#) encontraremos los diarios locales de diferentes ciudades y regiones de todo el mundo.
- Datos laborales, en páginas de las instituciones, ya que muchas personas no tienen cuentas en redes sociales o acceso a aplicaciones. Es muy común encontrar de listado de empleados con sus números de cédula en la Web, luego con esta información encontrar servicios como luz, agua, teléfono, la cadena de búsqueda es la que nos permitirá seleccionar la información.
- Generación de identidades para el proceso investigativo se recomienda realizar las investigaciones desde una identidad falsa, pero esta identidad debe ser creada con datos de otra persona, para este tema lo podemos hacer con [Fake Name Generator](#) para crear los datos de un individuo y [This person does not exist](#) para crear fotos falsas a partir de inteligencia artificial.
- **Buscadores:** muchos piensan que los únicos buscadores en Internet Google, Bing o Yahoo, pero existen otros buscadores como por ejemplo [Shodan](#) que nos sirve para buscar puertos o servicios publicados en Internet.

Le invito a visitar el sitio [Las mejores herramientas para la inteligencia de código abierto \(OSINT\)](#), el tema es muy amplio. Como un pequeño ejercicio usted puede ir al sitio [Twitter Analytics](#), colocar su usuario de Twitter y podrá determinar mucha información que está disponible para todos los usuarios de la Web y que muchas veces no sabemos.



Para concluir con este apartado (Pastorino, 2019) textualmente nos dice: “El universo de OSINT es sumamente grande y resulta imposible plasmarlo en una única investigación. Además, durante el workshop comprendí lo interesante que puede ser y las múltiples herramientas que existen para encontrar información. Como usuarios, debemos comprender la importancia de nuestra privacidad y sobre todo estar atento a que nuestra información no sea utilizada en nuestra contra”.

Troyano: instala programas espías dentro del computador afectado, para realizar acciones en él como: manejo remoto, cambio de archivos, robo de información, captura de datos personales, entre otras. Los troyanos son instalados a través de archivo infectados que pueden ser instalados en archivos adjunto a un correo electrónico también pueden ser insertados al momento de realizar una descarga de juegos, aplicaciones, etc. Es por eso que se debe realizar la descarga desde sitios del proveedor.

Por ejemplo, si queremos descargar un software cualquiera, para este ejemplo un reproductor multimedia libre y de código abierto (usuarios con experiencia pueden hacer cambios del código fuente y actualizaciones de acuerdo con la necesidad).

Figura 32.

Pantalla de búsqueda con resultados de un sitio oficial y un sitio no seguro



Nota. Captura de internet.

Al realizar la búsqueda podemos encontrar 2 sitios, como se muestra en la figura 32 el primero que puede ser un poco más tedioso pues es posible que nos pidan registrarnos para poder enviar información publicitaria y el segundo muy llamativo pues será la última versión y la descarga posiblemente será muy rápida, pero no garantiza la presencia de archivos maliciosos.

El objetivo de todos estos ataques es común, hacer caer los sistemas, generar terror cibernético, usurpación de información, buscar información que tenga valor y represente una ganancia para el atacante.

3.7. Tipos de ataque a los Sistemas de Información

De entre los ataques previamente listados, hemos escogido los siguientes para ampliar su información:

3.7.1. Ataque DOS

Los ataques de denegación de servicios (Denial of Service) son muy comunes en los SI. Consiste en enviar una cantidad elevada de solicitudes a un servicio de tal forma que el servidor que está brindando dicho servicio llega colapsar y cuando un usuario real del sistema quiere hacer su respectiva utilización no lo puede hacer porque el servidor está atendiendo las peticiones no válidas. En muchas ocasiones las peticiones del usuario real son rechazadas porque el servidor no avanza a cubrir todas las solicitudes hechas y genera información que no ha sido encapsulada correctamente. La red se satura por el excesivo tráfico con peticiones del atacante, ocasionando lentitud y tiempos de espera agotados, que se dan cuando no se ha logrado recibir una señal del destinatario.



Lo invito a revisar este [video](#) donde se realiza una explicación de este tema de forma muy ilustrativo

Los *firewalls* son la mejor solución para evitar este tipo de ataques, deben ser configurados para bloquear toda acción sospechosa como demasiadas peticiones que provienen de una misma dirección IP y a todos los usuarios que están haciendo peticiones extrañas, como peticiones de accesos a sitios no permitidos.

Las listas de control de acceso (LCA) ayudan a contrarrestar los efectos ocasionados por este tipo de ataques, pues nos permiten bloquear cierto tráfico y de direcciones sospechosas. Se puede configurar las LCA si se trata para uso interno con acceso a internet se debe bloquear todo el tráfico externo a excepción del proveniente por el puerto 80 que generalmente es del servicio de Internet.

Mencionaremos cuatro tipos de estos ataques:

- Ataque genérico de inundación o *flood*
- Ataques *smurf*
- Ataque *nuke*
- Ataque DDos

De los ataques mencionados, el *smurf* es uno de los más peligros, ya que existen muchas herramientas para realizar estos ataques las mismas que podemos encontrar con facilidad en la Web. Además, en este caso se puede realizar el ataque por dos medios el primero es por una mala configuración del *router* (dejar las configuraciones de fábrica) y por la utilización de servidores DNS. Aunque parezca obvio la solución a este ataque es la de una buena configuración del *router* de la organización y el establecimiento de capas de seguridad para la autentificación y confidencialidad de los protocolos UDP y DNS.

3.7.2. Puertas traseras

Las puertas traseras son puntos de acceso a un sistema sin ser detectados, debido a que el creador de la puerta pudo haber dado ciertos privilegios y está entrando como un administrador del sistema. Estas puertas muchas veces son utilizadas con fines maliciosos, como el plagio de información y espionaje.

También las puertas traseras son creadas con fines de administración del sistema por parte del desarrollador del sistema y se vuelve un problema cuando el desarrollador o alguien que conozca de la puerta la explotan en su beneficio. No solo el desarrollador puede crear estas puertas, también existen programas que permiten su creación. En Internet se puede encontrar el código necesario o programas para crear una puerta trasera, si es que no se es un experto en este tema solo es cuestión de entrar en un *blog* de hackers y listo, ya se tienen las puertas traseras en los sistemas que se está desarrollado.

En Pichincha (2021), nos presentan algunos temas, el primero nos permite saber si tu computadora tiene una puerta trasera instalada, claro que esto no es completamente real, los *backdoors* son difíciles de detectar, ya que sus síntomas son los mismos que los de un virus. Se pueden considerar algunas de estas señales que permitirían relacionar la presencia de alguien en un equipo:

- Problemas de rendimiento del computador.
- Velocidad de navegación en internet es demasiado lento.
- Saltan cuadros de diálogo para actualizar información o ingresar contraseñas.
- Ventanas emergentes en tu computadora.

Así mismo podemos considerar estos consejos que nos presentan, con una semejanza que si en nuestras casas mantenemos las puertas cerradas en nuestros computadores deberíamos hacer lo mismo:

- Mantener actualizado la versión del sistema operativo y actualizaciones, puedes hacerlo buscan *actualizaciones automáticas*, configura de tal forma que se haga periódicamente y el reinicio del computador se lo haga en horarios fuera del trabajo si es posible.
- No abrir correos con links que no se conoce, o correos en donde piden datos, hay amenazas de publicación de fotos o videos o te advierten que la cuenta de una institución será bloqueada o suspendida.
- Aunque esto ya se explicó no está de más volverlo a mencionar, descarga siempre desde sitios oficiales: los programas o apps que instales deben ser descargadas de tiendas y páginas Web autorizadas.
- Actualización del antivirus y firewalls: estos programas se encargan de detectar, proteger o eliminar malware.

En este sitio [VulDB](#), usted podrá encontrar un listado de algunas vulnerabilidades de este tipo, así como información estadística de problemas de seguridad, lo invito a revisar este sitio.

3.7.3. Overflows

Uno de los problemas más comunes de seguridad en lenguajes como C o C++ han sido los *overflows* (desbordamientos de memoria) que consiste en sobrepasar la capacidad de cálculo o exceso de datos en una variable, esto

por lo general es un error de programación, lo que conlleva a un problema de seguridad cuando el desbordamiento es producido intencionalmente por alguien que envía datos que incluyen porciones de código que son ejecutadas posteriormente.

Los overflows eran una de las vulnerabilidades más explotadas por los atacantes a un sistema de información, el gusano Morris es un ejemplo de ello. El gusano Morris fue el primero autorreplicable, su objetivo era averiguar las credenciales de otros computadores, aprovechando dicha vulnerabilidad.

Una solución a este problema de seguridad es la utilización de lenguajes de alto nivel (c#, Java, etc.) en cuyas plataformas ya tiene controlado estas situaciones, por lo que el programador no debe preocuparse por estas situaciones, donde el control de la ejecución lo tiene el lenguaje, en el caso de Java, su máquina virtual o en .Net el Framework, porque abstraen el acceso a memoria. A diferencia de C donde el programador tiene más control de cada una de las sentencias que escribe y es el mismo quien debe encargarse del control de estos problemas de seguridad.

3.7.4. Virus

Los programas maliciosos más conocidos son los virus, los cuales son software que produce un mal funcionamiento de los sistemas, ocasionando lentitud en la ejecución de procesos, errores en la ejecución del sistema operativo, abren o cierran puertos, anulan servicios, ocupan memoria, ejecutan acciones no deseadas y permiten un fácil plagio de información. La mayoría de los virus tienen este fin.

Un virus por lo general tiene tres funciones principales, las cuales son: ocasionar un daño, autoprotección, reproducción o expansión. Si no tiene una de las operaciones antes mencionadas no se lo puede catalogar a un programa como un virus. Existen varios tipos de virus como:

- **Los gusanos:** que son programas que se expanden por cualquier medio de transferencia de información ya sea discos extraíbles, red, etc.
- **Los troyanos:** los cuales se expanden escondiéndose en otros archivos como imágenes, archivos adjuntos de mail, cuando se expanden por

un mail por lo general el asunto del mail es algo que llama la atención, por ejemplo: *Has ganado un millón de dólares*, etc.

- **Las bombas de tiempo:** son otra forma de virus, estas bombas están programadas para que se ejecuten en una determinada fecha como un viernes 13, por lo general estas fechas son con un significado especial, ya sea una fecha de celebración nacional como el cuatro de julio u once de septiembre, o una fecha con un valor sentimental como el catorce de febrero o el veinticinco de diciembre.
- **Malware:** según (Aslan & Samet, 2020) nos dice que "Los delincuentes generalmente utilizan software para lanzar ciberataques a las máquinas víctimas. Ningún software que ejecuta intencionalmente cargas útiles maliciosas en las máquinas de la víctima (computadoras, teléfonos inteligentes, computadoras redes, etc.) se considera malware".
- **Ransomware:** es un tipo de malware que a partir de conseguir su objetivo de infectar a un determinado equipo secuestra la información a través de algoritmos de encriptación de información. Uno de ellos es el llamado WannaCry, (Akbanov et al., 2019) en su estudio explica: El 9 de febrero de 2017, investigadores de Fortinet descubrieron la primera muestra de WannaCry, que denominaron versión beta del ransomware. Esta versión encriptaba archivos usando el algoritmo AES-128 y no tenía ningún gusano componente implementado. El 28 de marzo de 2017, los mismos investigadores encontraron otra versión mejorada llamada WannaCry 1.0, que utilizó un diccionario codificado para acceder a las carpetas compartidas del bloque de mensajes del servidor (SMB) y soltó un navegador Tor enlace de descarga en el archivo cfg.

Todo software malicioso ocasiona algún daño por lo tanto siempre es necesario eliminar todos los virus con el fin de evitar cualquier problema.

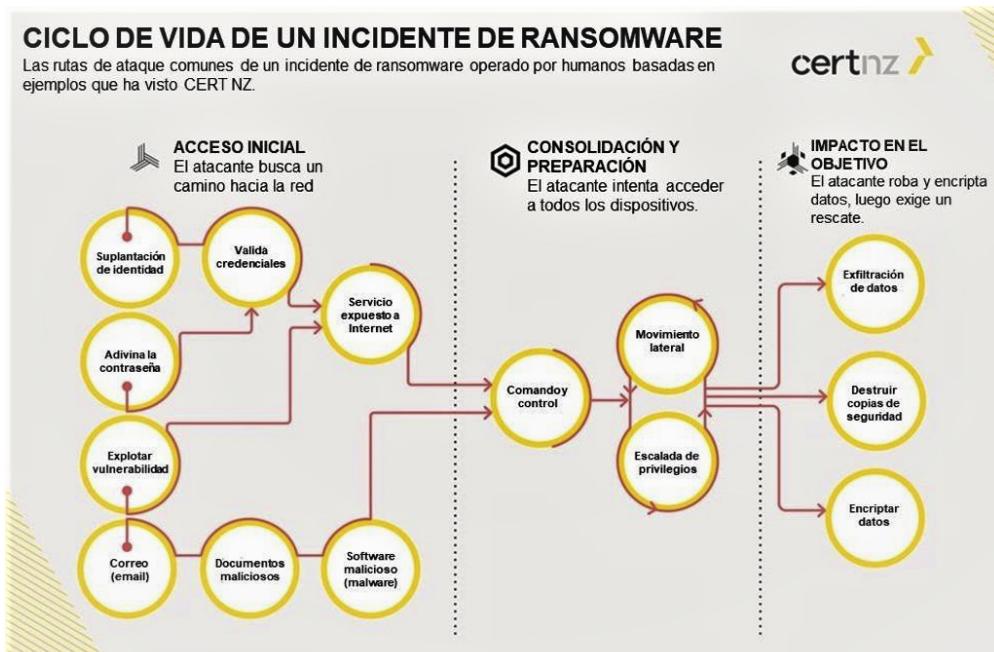
La mejor solución para eliminar virus es tener siempre un antivirus actualizado, no es recomendable tener más de un antivirus debido a que pueden causar algún conflicto entre ellos, cuando existe estos conflictos con antivirus el computador puede volverse exageradamente lento.

En la actualidad existen ya algunas empresas que ayudan a solucionar el problema del ransomware. Usted puede buscar en Twitter el hashtag

#NoMoreRasom y podrá encontrar algunas iniciativas como la de @Europol, se puede establecer contacto con esta empresa en el caso de sufrir este tipo ataque.

En el siguiente enlace podemos encontrar algunas consideraciones sobre rasomware. En el sitio del CertNz podrá encontrar el enlace que se ha utilizado para adaptar la figura No. 33 sobre el ciclo de vida de un rasomware:

Figura 33.
Ciclo de vida de un rasomware



Nota. Adaptado de Cert.govt.nz, 2021.

El proceso inicial empieza con procesos de ataque social como son phishing, email falso, a través de los servicios que han sido expuestos en el Internet que permita instalar un malware en el equipo. En el segundo punto se intenta pasar a escalar los privilegios del sistema y poder tomar el control de este. Finalmente, como podemos notar antes de realizar el proceso de encriptación para luego pedir un rescate los atacantes buscan los respaldos que se pueda tener para destruirlos.

3.7.5. Espías

Los espías son softwares que permiten el plagio de información de un computador. Los espías están monitoreando todo movimiento que se hace y lo almacenan en un archivo, por lo general guardan toda información ingresada por teclado, como usuarios de correos o cualquier otro sistema, claves, direcciones de correo, etc., en fin, los espías capturan toda la información ingresada y luego es enviada a la persona que está espiando (instalo el espía).

Existe una gran variedad de espías, estos por lo general vienen escondidos en programas, como reproductores o que ayudan a hacer ciertas funciones del sistema (Control de volumen, funciones de red) y programas en general. Al estar escondidos en el software, se ejecutan y no nos percatamos de que se trata de un espía, porque aparentemente es un software común y corriente el cual nosotros lo estamos utilizando con total normalidad.

Existen antiespías que permiten bloquear este tipo de programa, fáciles de descargar de internet y son gratuitos. También la gran mayoría de antivirus poseen estas funcionalidades que nos ayudan a estar protegidos.

¿Qué le pareció el tema?, si cree que es interesante, en la WEB hay mucha información sobre el mismo, como informáticos debemos profundizar acerca de estos contenidos. Le recomiendo realizar la *Actividad 2* al final del capítulo.

Le invito a profundizar sus conocimientos acerca de los tipos de ataque a los sistemas de información.

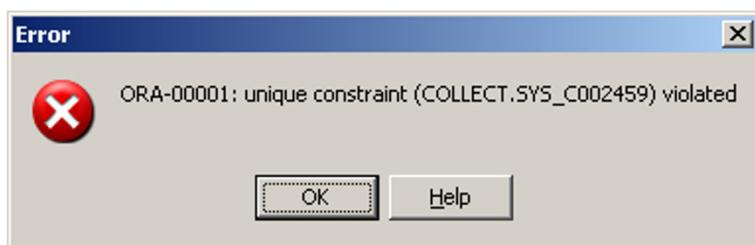
3.7.6. Excepciones no controladas

Una excepción es la ejecución de un proceso de una forma inesperada que ocurre debido a una situación que no se tiene prevista o no está debidamente controlada de allí el término “las excepciones son condiciones excepcionales que pueden ocurrir dentro del programa durante su ejecución” (Zator, 2016), ya que muchas veces no se está preparado para este comportamiento llevando un error del sistema y no se continúa con la ejecución normal del proceso. El no capturar una excepción es una vulnerabilidad del sistema, ya que al ser lanzada la excepción envía consigo información del sistema y la razón de la excepción con una descripción detallada con nombres de variables, sus valores, si es una excepción

de base de datos lanza nombres de tablas o procedimientos donde se produjo la misma, toda esta información que puede ser aprovechada por una persona que desea atacar el sistema. Con toda la información que se presenta al ser lanzada la excepción de cierta forma lo que está dando es información para que un atacante pueda tener acceso al sistema. Muchos ataques se hacen generando excepciones y con la información que es presentada a través de la interfaz gráfica del usuario puede ser suficiente para un acceso normal al sistema (Ver figura 34).

Figura 34.

Error no controla. Exposición de información como la base de datos que se utiliza



En lenguajes como java la máquina virtual tiene un manejador de excepciones incluido, el cual se encarga de capturar la excepción, aunque el programador no haya escrito el bloque para capturarlas, por tal razón en java no se presentan las excepciones a través de la interfaz de usuario, lo que no ocurre en lenguajes como C Sharp o C. En estos lenguajes es necesario especificar los bloques para capturar una excepción cuando esta es lanzada (Palos, 2016).

Al capturar una excepción se puede dar el manejo adecuado ya sea personalizando los mensajes para que al usuario final solo llegue información útil de tal forma que sepa que es lo que debe hacer o simplemente guardando la excepción en un *log* para que luego sea revisada por el administrador del sistema y haga los correctivos necesarios.

Cuando un usuario común es el que está utilizando la aplicación y ocurre una excepción la cual no ha sido controlada, el usuario no sabrá qué hacer y su primera sensación va a ser que el sistema está con problemas o tal vez al usuario le cause una fuerte impresión de ese error dejándolo en shock por un momento. En cambio, si se trata la excepción de forma adecuada y presenta un mensaje personalizado el usuario va a saber qué es lo que debe

hacer. La captura de excepciones se la debe hacer por motivos de seguridad y la personalización de mensajes se le debe hacer por usabilidad.

Muchos ataques se ejecutan actualmente haciendo que el sistema genere errores y que dicho sistema arroje información para que el atacante pueda fácilmente introducirse al sistema. Esto se logra cuando las excepciones no son tratadas de forma adecuada. Se pueden manejar las excepciones a través de ciertos controles o condiciones, pero esa opción es poco eficiente porque hay que observar todas las posibilidades y muchas veces al código fuente se lo ensucia perdiendo claridad para su entendimiento. La manera eficiente de capturar un error es a través los bloques try catch (Palos, 2016).

La mejor forma de controlar las excepciones es tener siempre los bloques *try*, *catch* y *finalize* los cuales permiten capturar errores y tratarlos de la mejor manera, de forma que se muestre al usuario solo un mensaje personalizado y no el error como tal. A través de revisiones de código manual en los diversos métodos se puede verificar si los bloques *try* y *catch* están en la ubicación correcta y al error se lo trata de la forma adecuada. Cuando se presenta una excepción es recomendable presentar un mensaje dependiendo del tipo de excepción, también se puede presentar un mensaje estándar para las todas las excepciones y no presentar el error como tal. Es recomendable al error tratarlo a través de un log de tal forma que solo el administrador del sistema tenga el acceso y solo él pueda revisarlo para tomar las decisiones apropiadas para los correctivos referentes al caso.

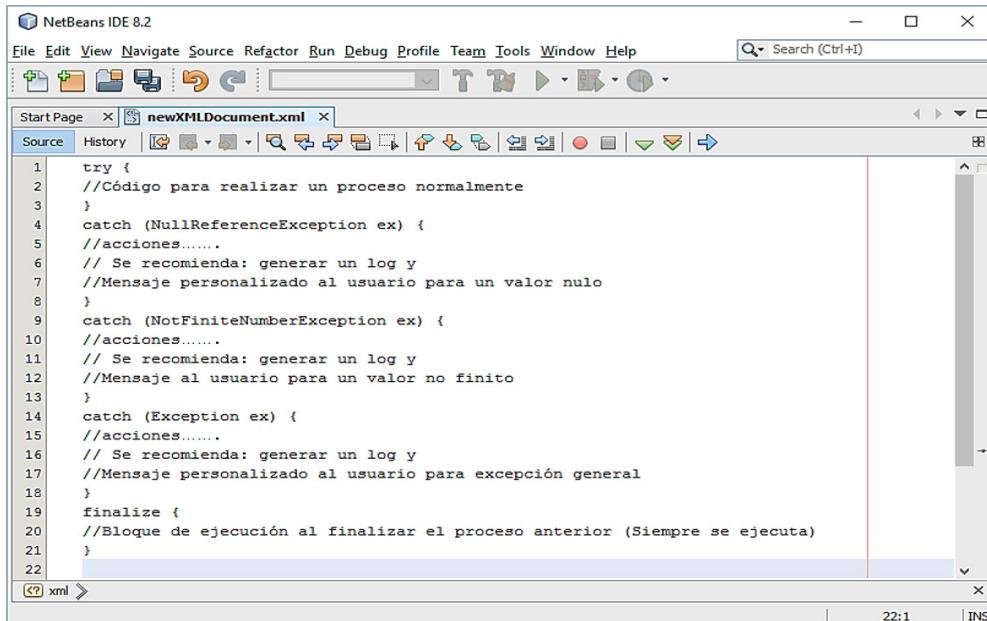
Existe la posibilidad que conozcamos que se vaya a producir una excepción en particular y podemos saber de qué tipo es esta excepción. Así que se puede capturar desde una excepción específica hasta una general. La excepción general siempre es la que va siempre al final, los bloques de captura de la excepción se ejecutan en el orden en que son colocados, siempre las excepciones particulares son las que deben ir primero y siempre la excepción general *Exception* debe ser la última en ser ubicada y luego de las excepciones va el bloque finalice el cual siempre se ejecuta independientemente de que se haya producido un error o no. Además, este bloque es opcional, se lo puede colocar como no. La figura 35 muestra un ejemplo en Java que permite el control de excepciones mediante el uso de *try* y *catch*.

La captura de excepciones permite tener un mejor control al sistema, permitiendo a este la tolerancia a fallos de tal forma que se pueda capturar

un error, disminuyendo así las posibilidades de explotar vulnerabilidades, como resultado se tendrá un sistema confiable.

Figura 35.

Ejemplo de un bloque try catch



The screenshot shows the NetBeans IDE interface with the title bar "NetBeans IDE 8.2". The menu bar includes File, Edit, View, Navigate, Source, Refactor, Run, Debug, Profile, Team, Tools, Window, Help, and a search bar "Search (Ctrl+I)". Below the menu is a toolbar with various icons. The main workspace shows a Java file named "newXMLDocument.xml" with the following code:

```
1 try {
2 //Código para realizar un proceso normalmente
3 }
4 catch (NullPointerException ex) {
5 //acciones......
6 // Se recomienda: generar un log y
7 //Mensaje personalizado al usuario para un valor nulo
8 }
9 catch (NotFiniteNumberException ex) {
10 //acciones......
11 // Se recomienda: generar un log y
12 //Mensaje al usuario para un valor no finito
13 }
14 catch (Exception ex) {
15 //acciones......
16 // Se recomienda: generar un log y
17 //Mensaje personalizado al usuario para excepción general
18 }
19 finalize {
20 //Bloque de ejecución al finalizar el proceso anterior (Siempre se ejecuta)
21 }
22
```

The code is annotated with comments explaining the purpose of each section. The bottom status bar shows "22:1" and "INS".

3.7.7. Acceso no autorizado

Los atacantes pueden llegar a utilizar un sinnúmero de estrategias como por ejemplo se ponen una corbata y crean una identificación falsa para entrar a las oficinas de la empresa como un empleado más. Como bastantes empresas implementan tarjetas de seguridad, los atacantes saben que las convenciones sociales son más importantes que la seguridad y esperan que algún empleado legítimo le *tenga la puerta* para poder entrar sin pasar por los controles de seguridad. Al tener acceso físico a las instalaciones es más fácil completar un ataque. Por ejemplo, dejar dispositivos como *keyloggers* o troyanos y hacer reconocimiento para realizar un ataque más especializado. El control físico a las instalaciones, por las personas que están en las recepciones, tienen que estar muy pendientes de que todos realicen adecuadamente el proceso de entrada.

3.7.8. La USB tentadora

Otra de las técnicas más conocidas y efectivas es dejar una USB en el parqueadero o en un sitio cercano a la oficina (como un café o un restaurante) para que algún empleado la lleve y la conecte a su computador. La USB, en principio, parece inofensiva, pero en realidad está cargada con malware que puede poner en peligro todo el sistema corporativo. Muchas compañías han deshabilitado los puertos USB de sus computadores, pero eso le quita bastante funcionamiento al equipo.

Es mucho mejor educar a los empleados y hacerles caer en cuentas las consecuencias que puede tener una vulnerabilidad informática.

Entonces, ¿qué debemos hacer?

Primero que todo, hay que tener en regla la tecnología. Los dominios.com.ec son de los más seguros del mundo y cuentan con la confianza de los empresarios, emprendedores e inversionistas. Por eso, para tener esa cuota de confianza en internet, te recomendamos registrar tu dominio en www.dominios.com.co. Debes tener un firewall de primera línea, todos los equipos deben tener el antivirus actualizado y tener un antispam dinámico e inteligente.

.ec se utiliza para referenciar un dominio en un nivel geográfico, este caso se utiliza para Ecuador, ejemplo: www.utpl.edu.ec, www.loja.gob.ec mientras que España utiliza es, así por ejemplo www.upm.es

Después, hay que hacer unas sesiones educativas con todos los empleados de la empresa. Los atacantes siempre van a buscar a la persona más débil para que los ayude con su objetivo. Por eso no puedes dejar a un lado a la asistente administrativa, al diseñador o cualquier otra persona que tenga acceso a los sistemas de la organización.

Es recomendable hablar con los empleados para explicarles el tema y darles ejemplos de posibles ataques. También debe haber un manual por escrito que deje claramente las mejores prácticas para prevenir la ingeniería social. No abrir enlaces de correos electrónicos desconocidos, devolver la llamada si crees que están suplantando la identidad de alguien y revisar bien las identificaciones de las personas caminando por las instalaciones

de la organización son unas buenas prácticas que puedes implementar inmediatamente para reducir el riesgo de ingeniería social.



Hemos terminado la unidad, estos temas son muy interesantes ¿Cómo le fue con su comprensión? Existió algunos temas que le resultaron familiares, es importante profundizar en aquellos temas que no han quedado claro. No dude en escribir a su profesor tutor por los diferentes medios de comunicación. Ayúdese de las tutorías para despejar sus dudas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

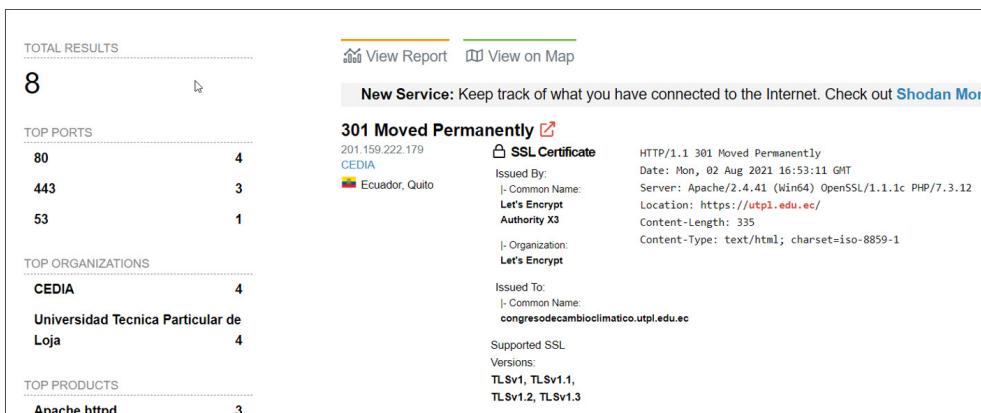
- Revise el link donde se puede revisar los [tipos ataque de ingeniera social](#) que en la actualidad están aumentando de forma acelerada
- En el enlace encontrará la [guía de ciberataques](#) propuesta por Incibe y OSI. Para que refuerce los conceptos tratados, de no poder conseguirla la puede ubicar en el EVA.

▪ Actividad 1:

Realice un trabajo de búsqueda de información:

- Búsqueda de información de un sitio Web, para ello podemos utilizar [Shodan](#).
- Si realizamos una búsqueda podemos encontrar información desde donde está el sitio y sus referencias desde otros, por ejemplo: [Enlace](#)

Figura 36.
Shondan



Nota. Tomado de [enlace web](#)

En la pestaña de *view report* podrá encontrar un mapa señalando en qué país está el sitio Web. A continuación, realice la búsqueda de un sitio que sea de su interés para poder determinar la información que presenta y donde está. Podrá ser utilizado para determinar desde donde posiblemente están tratando de realizarnos un ataque.

Realice la búsqueda de información.

■ **Actividad 2**

Spyware, muchas de las veces debemos conocer cómo funcionan para poder protegernos de los mismos. Le recomiendo visitar el sitio www.adslzone.net, en el mismo encontrará un listado de programas que se utilizan como espía. También se den algunas recomendaciones sobre el uso de estos programas en las empresas ya que podemos estar violando la privacidad de los empleados y eso está sujeta a sanciones. Muchas de las veces estos programas son utilizados como forma de hacer un control parental a nuestros hijos, hasta dónde podemos llegar es la pregunta.

Le recomiendo descargar de los sitios oficiales algunos de estos softwares y hacerlos funcionar, además debe ser analizado por el antivirus si está reconocido como un software espía o no.

Una vez que ha estudiado los conceptos relacionados con la Unidad 3, le invito a desarrollar la autoevaluación con el fin de evaluar los conocimientos adquiridos hasta el momento. Posterior a eso usted podrá encontrar al final de este texto guía la solución a cada una de las preguntas.

¡Éxitos en la autoevaluación!



Autoevaluación 3



Una vez que ha estudiado los conceptos relacionados a la unidad 3, le invito a desarrollar la autoevaluación con el fin de evaluar los conocimientos adquiridos hasta el momento. Posterior a eso, usted podrá encontrar al final de este texto-guía la solución a cada una de las preguntas.

¡Éxitos en la autoevaluación!

- 1. ¿En qué fase de un ataque se realiza la extracción de información para realizar el mismo?**
 - a. Reconocimiento.
 - b. Exploración.
 - c. Obtener el acceso.

- 2. La principal característica de la fase de exploración durante un ataque informático es:**
 - a. El establecimiento de estrategias mediante el aprovechamiento de las diferentes debilidades del sistema.
 - b. La materialización de la penetración al sistema mediante las vulnerabilidades encontradas.
 - c. La obtención de la información de la potencial víctima.

- 3. Entre los aspectos comunes a considerar a la hora de implementar un sistema de información tenemos:**
 - a. Solamente los aspectos técnicos.
 - b. Físicos, lógicos y de personal.
 - c. Ninguno de los anteriores.

4. En los ataque de tipo “intercepción”:

- a. Es un ataque contra la integridad, en el cual además de acceder a un recurso, se manipula su información.
- b. Es un ataque contra la confidencialidad en donde una entidad no autorizada consigue acceso a un recurso.
- c. Es un ataque contra la disponibilidad, en donde un recurso del sistema puede ser destruido o volverse no disponible.

5. El ataque de tipo “Cross Site Scripting (XSS)”:

- a. Se aprovecha de errores de programación para hacer que el servidor utilice sus recursos de manera indiscriminada hasta hacerlo colapsar.
- b. Consiste en dejar público el registro de errores, facilitando observar las fallas del sistema para tomar provecho.
- c. Se basa en la inserción de códigos o scripts en el sitio web para hacer que el usuario lo ejecute y cumpla el cometido para el cual fue escrito.

6. Se ha ejecutado un ataque de DoS donde se ha dejado inhabilitado el sistema, este ataque se lo puede considerar en forma general como un ataque de:

- a. Intercepción.
- b. Interrupción.
- c. Fabricación.

7. Tenemos la herramienta workbench que permite realizar la administración de base de datos. Dentro de un sistema de información esto se consideraría como:

- a. Hardware.
- b. Software.
- c. Middleware.

- 8. Luego de un proceso de auditoría en nuestro servidor, se determinó que se colocó un archivo falso en el sistema al mismo que no se puede determinar su autenticidad, es un ataque de:**
- a. Intercepción.
 - b. Interrupción.
 - c. Fabricación.
- 9. Consiste en suplantar la identidad del computador de una persona, mediante la sustitución de datos. Este es un ataque de:**
- a. Phishing.
 - b. Scam.
 - c. Spoofing.
- 10. Al no controlar el ingreso adecuado sobre un campo de texto de nuestra aplicación, se ha podido ingresar un script de ejecución, es un ataque:**
- a. DoS.
 - b. XXs.
 - c. OverFlow.

Puede verificar las respuestas de esta autoevaluación al final del Texto Guía.

[Ir al solucionario](#)

Si su puntaje no es bueno, es importante que vuelva a revisar los contenidos de la unidad y los recursos de aprendizaje, no olvide que puede interactuar con su tutor por cualquier medio de comunicación que brinda la UTPL para que aclare sus inquietudes.



Actividades de aprendizaje recomendadas

Estimado estudiante, estamos en la semana 8 de estudio de esta asignatura, prácticamente finalizando el ciclo académico y el primer bimestre. Es importante que esta semana usted haga el estudio de las unidades 1, 2 y 3. Así mismo, lea por favor las siguientes recomendaciones como preparación para la evaluación presencial o virtual:

Nota. Conteste las actividades en un cuaderno de apuntes o en un documento de Word.

- Haga una lectura comprensiva de los temas y subtemas estudiados en cada unidad. Puede utilizar algunas herramientas como resaltar, hacer resúmenes, mapas mentales, etc.
- Realice las actividades recomendadas en cada semana, tanto las calificadas como las que están expuestas como apoyo para reforzar conocimientos.
- Vuelva a desarrollar las autoevaluaciones.
- Si tiene alguna inquietud o duda respecto a las actividades práctico-experimentales, actividades de contacto con el docente o las de trabajo autónomo, por favor comuníquese con el tutor en los horarios establecidos o utilice los medios de comunicación antes expuesto.
- Esté atento a alguna comunicación sobre las evaluaciones que hacen desde la UTPL.
- Haga con tiempo algún trámite que necesita como para que pueda presentarse a las evaluaciones.
- Consulte el horario y lugar para rendir la evaluación presencial de la asignatura.



Segundo bimestre

Resultado de aprendizaje 6

- Explicar las diferencias entre los sistemas criptográficos simétricos y asimétricos y cómo los sistemas criptográficos ofrecen integridad, confidencialidad y autenticación.

Al iniciar este segundo bimestre es importante que usted relacione los conceptos de seguridad. Si aún existen dudas por favor revise el texto básico o contacte con su docente/tutor a través de los distintos medios como correo electrónico, plataforma virtual (EVA) o línea telefónica. En estas dos semanas de estudio nos centraremos en conceptos que se deben seguir para el desarrollo seguro de aplicaciones, así como mencionaremos algunas herramientas que nos permitan agilizar los procesos de aseguramiento.

Contenidos, recursos y actividades de aprendizaje



Semana 9

Unidad 4. Desarrollo seguro de aplicaciones

Estimado estudiante empezamos el estudio de esta unidad que es de vital importancia, por lo que lo invito a continuar con el mismo empeño revisando los diferentes conceptos y definiciones que aparecerán a continuación.

Esperamos que los temas que se trataron en la unidad anterior estén comprendidos a plenitud, si no sucedió así recuerden que ustedes pueden acceder al EVA para plantear las interrogantes que considere necesarias a su profesor tutor. Si bien es cierto, la unidad tres abarca temas como son el de establecer niveles de seguridad y mecanismos de control de acceso, siendo estos relevantes a la hora de implementar un sistema de seguridad en la organización, permitiendo establecer de cierta forma las personas autorizadas para acceder a un sistema en común y realizar las operaciones que hayan sido asignadas.

Iniciemos este estudio con el siguiente tema, teniendo en cuenta las instrucciones detalladas a lo largo del desarrollo de esta unidad.

¡Éxitos en el estudio de esta unidad!

4.1. Importancia del desarrollo seguro de aplicaciones

Debemos empezar considerando que ningún *software* es seguro, por lo tanto, una vulnerabilidad se considera un posible error de programación en el *software* que es explotada por un intruso con la finalidad de tener acceso a nuestro sistema, en la mayoría de los casos para dañar el mismo. Se debe considerar que a mayor grado de exposición de la información a través de procesos digitales de las empresas, mayor es el grado de exposición y que intrusos intenten acceder a nuestra información. Ante esta exposición de información a las diferentes amenazas que se presentan es necesario proteger los activos de la organización, entonces es común que también escuche el concepto de Ciberseguridad. La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan con la finalidad de proteger la información que se procesa en computadoras, dispositivos móviles, servidores, sistemas de redes y otros, es decir, que están en el ciberespacio.

Se debe considerar que para lograr que la infraestructura de TI que deseamos implementar se diseñe considerando las amenazas a las que nos podemos enfrentar, es importante también que las personas involucradas en el proceso de implementación estén conscientes de estos problemas. En la actualidad es imposible conocer todas las vulnerabilidades que se han desarrollado, así como los ataques que se han dado. Las vulnerabilidades en las aplicaciones pueden dividirse en aquellas. Las vulnerabilidades más explotadas las podemos ubicar en [OWASP](#), el mismo que es un proyecto de código abierto que nos ayuda a determinar las causas que hacen que el *software* sea inseguro.

Todos estos procesos se pueden lograr asegurando el desarrollo de las aplicaciones de forma segura, así como existe una metodología de desarrollo de software, también existe el ciclo de vida de desarrollo seguro de software, es decir, qué tenemos que hacer con respecto a la seguridad según sea la etapa en la que nos encontremos.

Los problemas de seguridad (vulnerabilidades en el software) por lo general son causados por fallas en la programación, es decir, malos programadores o equipos de desarrollo que no tienen la suficiente experiencia en el desarrollo seguro de aplicaciones. Por ejemplo, la falta de captura de una excepción, la falta de validación en el control de sesión al abrir nuevas páginas, etc.

Así podemos encontrar algunos procesos de desarrollo seguro que nos pueden ayudar en el desarrollo seguro de aplicaciones, dejaremos aquí el listado de algunas metodologías y frameworks de trabajo como Microsoft – Security Development Live Cicle, OWASP – Software Assurance Maturity Model o el framework Spring Security,

Algunas consideraciones que debemos tener:

- Colocar mecanismos de autentificación que no puedan saltar, estos deben ser colocados desde el inicio de la aplicación, es muy común por temas de tiempo obviar esto al inicio que al final termina sin ejecutarse.
- Se deben siempre actualizar la configuración por defecto, sistemas operativos, bases de datos, servidores de aplicaciones Web, servidores Web, etc., así por ejemplo el usuario por defecto de un Sql <>sa; pwd=123>> que, aunque no se crea, es casi lo que primero busca un atacante.
- Los privilegios o permisos de acceso deben ser entregados únicamente a quienes los necesiten ya sea con respecto a base de datos o sistema operativo, pues al momento de poner en producción una aplicación estos no son corregidos y seguirán por mucho tiempo.

Podemos entonces definir algunas ventajas que nos permitirán el desarrollo seguro de aplicaciones:

- Detección de fallos en el sistema de forma temprana.
- Reducir los costos que implicará colocar seguridad cuando el sistema ya esté en funcionamiento.
- Resolución de problemas de forma temprana.
- Minimizar el riesgo en problemas de seguridad dentro de la organización.

Le recomiendo revisar este sitio donde se puede revisar los requerimientos para realizar un proceso de certificación en [ICS](#) no es el único, puede buscar otros en la Web.

El desarrollo de aplicaciones en la actualidad ha tomado nuevas formas de realizarlo, pues las herramientas y lenguajes de programación están en una evolución constante. A continuación, se presenta una infografía sobre aspectos que deben ser considerados como temas actuales en el desarrollo de aplicaciones. Ver documento [Pila de desarrollo completa](#).

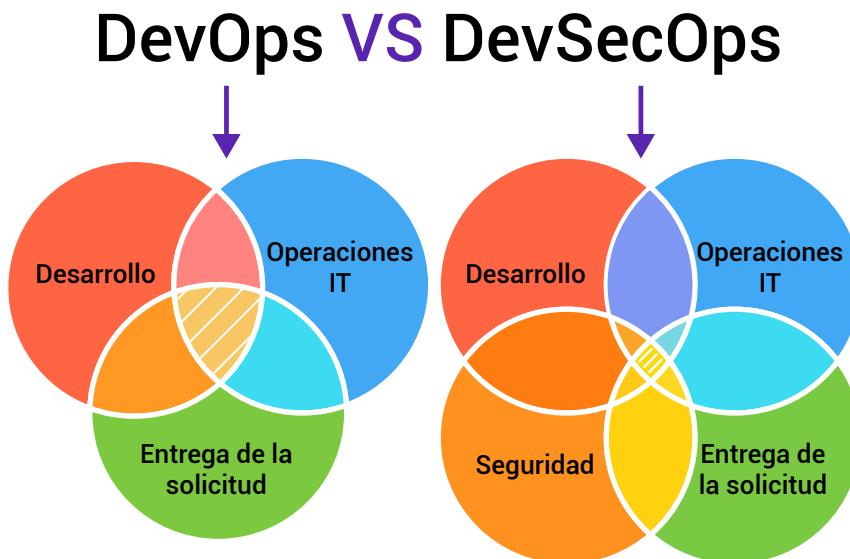
Se muestran algunas herramientas, esto no quiere decir que un desarrollador debe tener el conocimiento de todas estas herramientas, lo que debemos es considerar el uso de las mejores herramientas y conocer los aspectos que estas presentan con respecto a la seguridad. Entonces debemos pasar a un trabajo de mayor aplicación, puesto que en la actualidad se proporciona un sinnúmero de herramientas para el desarrollo.

Ahora le recomiendo realizar la *actividad 1* para profundizar en los temas tratados.

En la actualidad se está hablando mucho el tema de DevOps y DevSecOps como se muestra en la figura 37.

Figura 37.

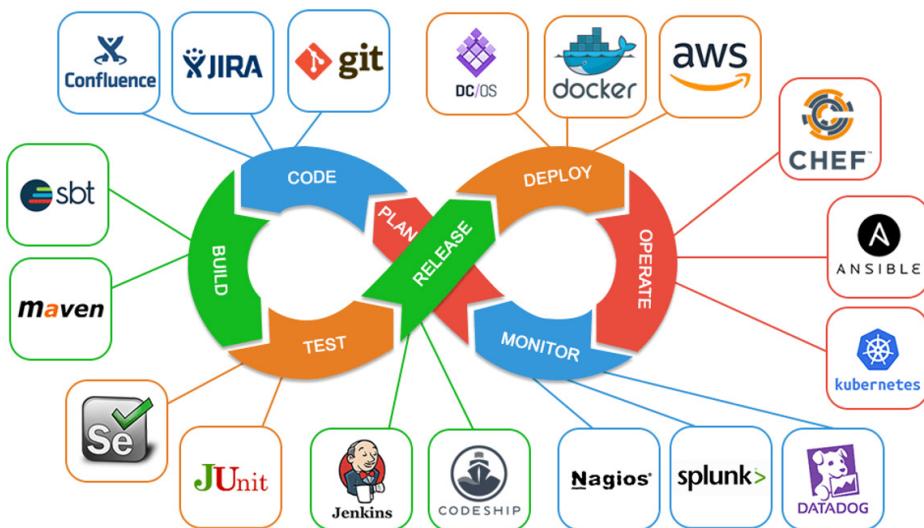
Comparativa de fase entre DevOps y DevSecOps



Nota. Tomado de *Máquinas Virtuales*, 2021.

Para el tema de DevOps nos permite la integración de metodologías ágiles en el desarrollo, pues hacemos la entrega continua, sobre este tema no vamos a profundizar solo señalar la integración de que las áreas de desarrollo de aplicaciones y el área de operaciones de TI estén constantemente colaborando entre ellas. Esto permitirá que al momento de lanzar a producción aplicaciones que están siendo desarrolladas por separado o varios equipos se permita una intersección entre todos y se llegue a cumplir el objetivo común de la organización. En la figura 38 nos permite ver ciclo de vida que se lleva y en cada de estas fases que herramientas podemos utilizar, señalando que no es necesario que se utilicen todas las herramientas.

Figura 38.
Pipeline de uso de herramientas en DevOps

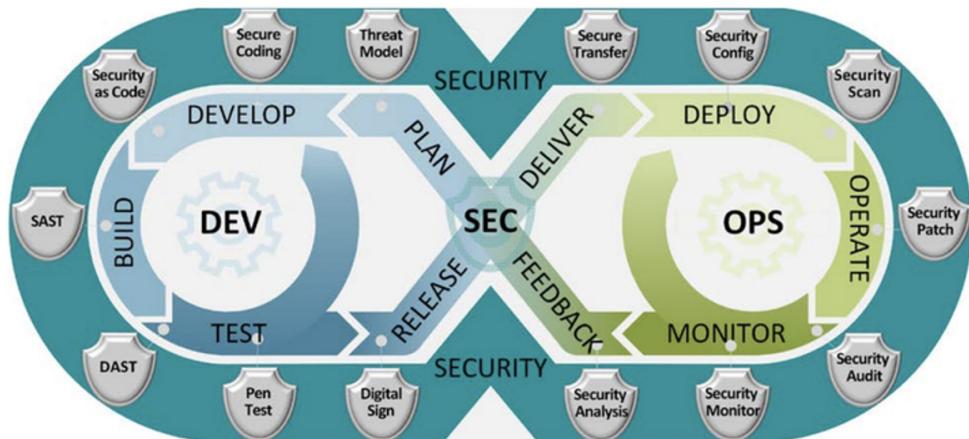


Nota. Tomado de [enlace web](#)

En la parte de DevSecOps, como se mostró en la figura 38, se integra a este ciclo de vida de desarrollo de aplicaciones, el componente de seguridad. Como podemos ver hay temas de análisis de la seguridad, codificación segura, pruebas de penetración, configuración de la seguridad y parches de seguridad, es decir, temas tanto de desarrollo de aplicaciones como de operaciones.

Figura 39.

DevSecOps



Nota. Tomado de [SEI, 2021](#).

Como podemos notar en cada una de las fases que estamos trabajando existe una parte de seguridad que debe ser considerada, concluyendo entonces que la seguridad no debe ser parte al momento de poner en producción una aplicación sino igual que todo debe ser considerada desde la fase inicial hasta la fase final.

En la tabla 24 se realiza una explicación por cada una de las fases tanto en Develop como Operations y la actividad que se debe realizar respecto a la seguridad con una breve descripción.

Tabla 24.

Actividades DEV/SEC

Fase: Dev/Sec	Actividades	Descripción
Plan	Modelo de amenazas	Identificar y enumerar las amenazas posibles
Develop	Codificación segura	Utilización de estándares de programación
Build	SAST (Static Application Security testing)	Pruebas de seguridad de análisis estático mediante revisión de código
Test	DAST (dynamic applications Security testing)	Pruebas de seguridad dinámicas, la aplicación funcionando (en entornos de prueba y producción)
Release	Digital sing	Mecanismo criptográfico para verificar la comunicación entre las partes
Deliver	Transferencia Segura	Utilización de protocolos seguros de comunicación

Fase: Dev/Sec	Actividades	Descripción
Deploy	Configuración Segura	Consideraciones sobre la configuración de <i>hardware</i> y <i>software</i> sobre sus parámetros iniciales
Opérate	Parches de seguridad	Actualización de versiones
	Auditoria de seguridad	Accesos en la organización del <i>hardware</i> y <i>software</i>
Monitor	Monitoreo de la seguridad	Cambio en estados de los dispositivos Cambios de <i>hardware</i> y eliminación de datos del sistema
Feedback	Análisis de la seguridad	Que pasó, cómo corregirlo, riesgos, nuevos controles.

A continuación, vamos a tratar algunos de los elementos esencial que son necesarios para el desarrollo de aplicaciones con relación a la seguridad y que deben ser consideradas en cada fase. Es importante profundizar en estos temas dentro de la organización.

4.2. Requisitos de Seguridad

El proceso de levantar los requisitos de seguridad se realiza mediante un proceso donde previamente se deben identificar los riesgos de seguridad que encontramos. Cuando se desarrollan aplicaciones los requisitos de seguridad se consideran como requisitos no funcionales, estos se deben seleccionar.

Debemos considerar que en la actualidad la seguridad ya cuenta con el apoyo de quienes dirigen los proyectos pues se ha visto que estos requisitos deben ser implementados desde la concepción misma del sistema a desarrollar.

Un ejemplo que era muy común antes, la seguridad de las aplicaciones eran únicamente el usuario y *password*, con eso la aplicación comenzaba su funcionamiento y luego debía irse incorporando de acuerdo a las necesidades por ejemplo la complejidad de la contraseña. Eso involucraba que cuando se hacía la actualización los usuarios tenían que generar nuevas contraseñas, pero no se adaptaban a las reglas que se definían. Otro problema era que se permitía estar probando por contraseñas de usuarios sin ningún control entonces había procesos que comenzaban a hacer un minado de esas claves (ataque por fuerza bruta) buscando una infinidad de combinaciones, entonces se tenían que nuevamente realizar parches o

nuevas versiones relacionadas con la seguridad, pero hasta que esto ocurría ya existían algunos procesos críticos que eran explotados por usuarios mal intencionados.

Como uno de los requisitos esenciales se debe identificar datos sensibles y cómo los vamos a gestionar, pues resulta difícil implementar mecanismos de seguridad si no tenemos claro que es lo que se debe cuidar, pues no vamos a implementar por ejemplo procesos de encriptación de datos para todos los datos, sería imposible. Esto es importante para poder empezar el proceso de diseñar la seguridad desde el comienzo del proceso de desarrollo seguro de aplicaciones. Otras de las consideraciones que se debe realizar es el de no transferirle al usuario del sistema el proceso de seguridad, es decir, que hacemos una funcionalidad y vamos a capacitar al usuario final para que no cometa errores, pero puede ser que ese proceso no se lo pueda hacer con todos y en el tiempo indicado por lo tanto el problema existirá. Debemos considerar que si a un usuario se le dice *no lo haga* él por curiosidad lo hará.

Requisitos no Funcionales

Según (Ecured, 2018), “son requisitos que imponen restricciones en el diseño o la implementación como restricciones en el diseño o Estándares de Calidad. Son propiedades o cualidades que el producto debe tener”. De la misma manera (Yenisel et al., 2019), los considera como “requerimientos de calidad, que representan restricciones o las cualidades que el sistema debe tener tales como: precisión, usabilidad, seguridad, rendimiento, confiabilidad, performance entre otras. Estos requisitos poseen una naturaleza abstracta e intangible en comparación con los RF y esto hace que sean más difíciles de especificar o documentar formalmente. No alteran la funcionalidad del sistema, pero pueden añadir nuevos RF”.

De esta forma existen diferentes categorías de los requisitos no funcionales entre ellas requisitos de:

- Apariencia
- Usabilidad
- Rendimiento
- Mantenibilidad y portabilidad
- Seguridad
- Culturales y políticos
- Legales, entre otras

Es así que los requerimientos de seguridad catalogados como no funcionales permiten establecer temas como:

- Sistema operativo correctamente actualizado
- Servicios de comunicación red seguros
- Implementaciones de mecanismos de seguridad
- Implementación de doble factor de autenticación
- Contrasenñas seguras
- Autenticación cifrada
- Control de sesiones
- Algoritmos de encriptación
- Etc.

La aplicación no debe permitir que un mismo usuario tenga varias sesiones activas. ¿Qué tipo de requerimiento es? Funcional o No funcional.

4.3. Diseño Seguro

En la actualidad las aplicaciones se constituyen por sistemas complejos, es decir, ya no estamos hablando de un servidor de datos al que se accede desde un aplicativo, sino que involucran componentes diferentes interactuando entre sí, ya podemos encontrar entonces sistemas externos financieros que nos ayudan a realizar pagos, o sistemas estatales para búsqueda de información. De esta forma cada vez que se realice un cambio en el sistema el panorama de seguridad pueda cambiar y tendremos que volver a evaluarlo, aquí cabe señalar la integración que se deben dar entre las áreas de trabajo. Es decir, desarrollo y tecnología, la forma de realizar y analizar los sistemas debe pensarse en forma general.

La integración de componentes va a cambiar el entorno a un posible ataque, dichos componentes debemos analizarlos de manera unitaria y en conjunto considerando cómo se combinan, cómo se van a mantener o reemplazar en un determinado momento. Entre el 70% y el 90% de las aplicaciones Web tienen vulnerabilidades debido a que los desarrolladores no han seguido un proceso de formación adecuado.

Es importante considerar los requerimientos no funcionales que se han levantado para el proyecto, pues se debe entender el ambiente en donde se implementará la aplicación, debemos partir de la identificación y documentación de los riesgos, así como la priorización de estos. Pues no

siempre es lo mismo hacer el desarrollo de un sistema para una institución educativa que para una institución bancaria, entonces no en todos los sistemas debemos colocar los mismos mecanismos de seguridad, porque los costos de la implementación de la seguridad también van a cambiar. Muchas de las veces esto es lo que impide colocar dichos mecanismos en la seguridad.

Al identificar las amenazas de forma correcta podemos prevenir defectos en el diseño de la aplicación referente a la seguridad, es decir, vamos a concientizarnos de los riesgos que podemos encontrarnos. Recuerde que a mayor número de mecanismos de seguridad que coloquemos también el tiempo de respuesta puede subir. Por ejemplo, si hacemos muchos procesos de encriptación de los datos al momento de recuperarlos necesitaremos los mismos procesos de desencriptación entonces no todo debe estar encriptado. Debemos realizar un diseño acorde al entorno donde nos desarrollamos.

Aquí también es importante saber con qué herramientas podemos contar, por ejemplo, si vamos a utilizar un recurso externo para pagos debemos hacerlo con aquellos que ya son probados y dejar la seguridad en manos de ellos. Por ejemplo, es mejor utilizar servicios Web de aplicaciones de cobro, que hacer desde el principio una para utilizarla. Se deben consumir esos recursos.

Por ejemplo existe el estándar de cumplimiento PCI-DSS (Payment Card Industry Data Security Standard, o Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago) para operar el servicio de tarjetas de crédito en las aplicaciones Web, el [helpSystem](#) le ayudará a entender más sobre este tema.

Como resumen podemos colocar algunos principios

- El mínimo privilegio
- Hacer lo más simple las cosas
- Mantener la privacidad de los datos
- Segregación funcional
- Asegurar el eslabón más débil
- Implementar la seguridad en todas las capas
- No dejar procesos de seguridad en cuanto a usuario final

4.4. Codificación Segura

Muchas de las veces confundimos términos al momento de realizar la construcción de aplicaciones, las llamadas sesiones de trabajo para revisión de código están destinadas a la forma de la programación, es decir, se revisan aspectos como nomenclatura de variables, métodos, procesos. Así también aspectos relacionados con una forma correcta de escritura es decir mantener la identación (tabulación), la utilización de formato correcto en las palabras de cada lenguaje y este tipo de aspectos.

Entonces nosotros debemos ir un poco más allá en la revisión de código con respecto a la seguridad, como sería la entrada de datos, utilización correcta de parámetros.

En este apartado podremos ayudarnos de algunos marcos de trabajo como el [Marco de conocimientos de seguridad de OWASP](#) el mismo que al ser de código abierto permite tener información de cómo realizar el proceso de codificación segura en varios lenguajes de programación.

Herramientas de revisión de código:

- Review Board
- Crucible
- GitHub
- Phabricator
- Collaborator
- CodeScene
- Visual Expert
- Gerrit
- Rhodecode
- Veracode
- Reviewable
- Peer Review for Trac

Un punto muy importante es no dejar al usuario final temas de seguridad, por ejemplo, decir en el cuadro no debe ingresar caracteres especiales, no el programa debe contar con controles de entrada con respecto a capa de presentación, de esta manera debemos autorizar lo que se pueda hacer y denegar todo aquello que no corresponda. Esto se realiza con la finalidad de que un atacante pueda en esos datos colocar o interpretarlo como lenguaje de programación para poder manipular el sistema.

Una buena práctica para esto es la realización de componentes comunes que se mantienen en un repositorio y que deben ser utilizados por todos los programadores.

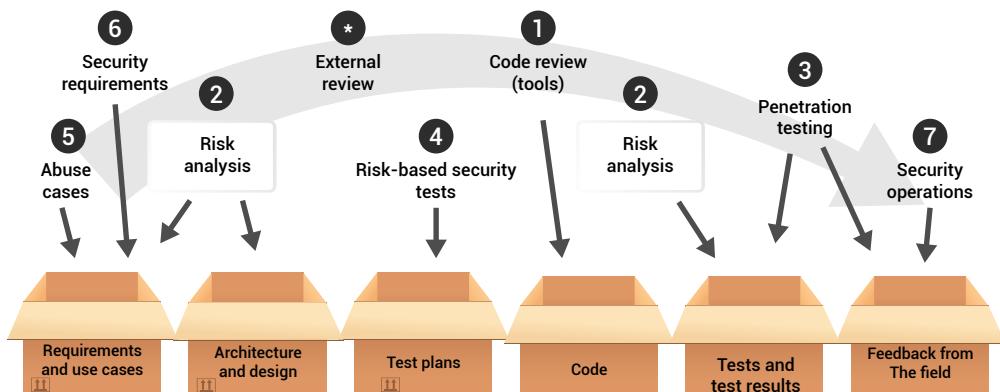
Existen muchos estándares de programación segura que se deben considerar el momento de la construcción de una aplicación, estos no deben estar separados del proceso ni tampoco deben incluirse al final pues casi siempre no se los colocara.

Para una mejor comprensión del tema, realice la *Actividad* en las actividades de aprendizaje recomendadas.

4.5. Los touchpoints de seguridad del software durante el ciclo de vida de Sistemas

Los *touchpoints* son un conjunto de buenas prácticas para seguridad del software, en el orden. En el texto (McGraw et al., 2011) sobre el desarrollo seguro de aplicaciones explica:

Figura 40.
Touch point de la seguridad de software



Nota. Tomado de MacGraw, 2010.

Aquí podemos encontrar algunos elementos como son las pruebas de penetración y su importancia como lo explican en (Correa et al., 2021). Además, ahora explicamos algunos de esos puntos esenciales que son mencionados por MacGraw.

Revisión de código

Puesto que la mayor parte de ataques de penetración a los sistemas se dan por este camino, en el código, la atención debe enfocarse a la revisión de errores, especialmente con aquellas herramientas de análisis estático que escanean el código para descubrir vulnerabilidades. Unos de los ejemplos más clásicos son: Buffer overflow on line NN, que se presenta principalmente en lenguajes como C y C++, este último con mayor porcentaje que el primero.

La revisión de código es necesaria, puesto que ayuda a determinar problemas de software, pero no es suficientemente eficaz como para mejorar la práctica segura de software. Las siguientes son herramientas para análisis estático e identificación de métricas de software:

- [Sonarqube](#) en su versión de prueba. Este software además de testear las buenas prácticas de código también ayuda en los aspectos de seguridad.
- Kiuwan.
- Codacy.

Arquitectura de análisis de riesgos

Diseñadores, arquitectos, analistas y debería documentar claramente los supuestos e identificar los posibles ataques a la aplicación. El omitir esto no permitirá que los mecanismos de seguridad sean aplicados.

Ejemplos de los riesgos encontrados: la protección de los datos críticos, fracaso de un servicio Web para autenticar una llamada, control de acceso basado en contexto.

Pruebas de penetración

Las pruebas de penetración son útiles, especialmente si una arquitectura de análisis de riesgos ha de informar sobre estas pruebas. La realización de estas pruebas de penetración nos da una ventaja en tener una buena comprensión de los programas informáticos sobre el terreno en su entorno real donde se van a desarrollar. Medir en lo posible las fugas de datos, tomando en consideración el riego en la protección de datos, podría ser un ejemplo.

Le recomiendo realizar una búsqueda de herramientas para realizar pruebas, por ejemplo, tenemos pruebas unitarias en [Junit-*http://junit.org/junit4/*](http://junit.org/junit4/) como una herramienta. En el entorno virtual se cargará un video de cómo realizar las pruebas con Junit de un pequeño programa desarrollado. A nivel de JavaScript puede encontrar JestJS, que es un marco de prueba con un enfoque en simplicidad. Esta tecnología ocupa paquetes de Testing propias de NodeJs.

En el sitio [GURU99](#), se nos presenta un listado de herramientas que nos permiten realizar pruebas de penetración, como: Netsparker, Acunetix, Intruder, entre otras, con los links a las mismas y una explicación, por lo que sería ideal que usted revise estas herramientas para que tenga una referencia de cada una de ellas.

Riesgos basados en las pruebas de seguridad

Un buen plan de pruebas debe contemplar también las estrategias. Las pruebas de seguridad deben abarcar: las pruebas de seguridad con la funcionalidad estándares de pruebas funcionales-técnicas y las pruebas basadas en el riesgo de seguridad las que deben basarse en pruebas patrón, de posibles ataques.

Casos de abuso

Los casos de abuso son una forma de poder determinar cómo se comportará un posible atacante del sistema. Similares a casos de uso, los casos de abuso del sistema deben describir el comportamiento en virtud de un posible ataque; la construcción de casos de abuso requiere la cobertura explícita de la data que debe ser protegida, de quienes y por cuánto tiempo.

Requisitos de seguridad

La seguridad debe ser trabajada explícitamente en cuanto a requisitos. Deben cubrirse tanto las necesidades de seguridad abierta como de seguridad funcional, aquí se puede mencionar el uso de la criptografía. Este tema fue explicado en un apartado anterior

Operaciones de seguridad

La seguridad del software se puede beneficiar en gran medida de la seguridad de la red. Estos dos elementos bien integrados permiten las operaciones de seguridad. Además de fomentar la seguridad de las redes

esta puede proporcionar la experiencia y la sabiduría de seguridad que de otro modo podría faltar en el equipo de desarrollo.

Los conocimientos adquiridos mediante la comprensión de los ataques deberían volver a un ciclo de desarrollo de software, para ser tomados en cuenta en los requisitos de seguridad.



Hemos terminado esta semana de trabajo. Estos temas son muy interesantes ¿Cómo le fue con su comprensión? ¿Existieron algunos temas que le resultaron familiares? Es importante profundizar en aquellos temas que no han quedado claros. No dude en escribir a su profesor tutor por los diferentes medios de comunicación. Ayúdese de las tutorías para despejar sus dudas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

- Revise los sitios:
 1. Oracle: Code Conventions for the Java TM Programming Language:
 2. [Oracle: Estándares de codificación](#)

En estos sitios podrá encontrar un detalle de los estándares de programación y codificación segura.

▪ Actividad 1

En el apartado 4.4 existe el listado de algunas herramientas para la revisión de código, seleccione alguna de ella y realice la instalación, configuración y ejecución para revisar el código de la aplicación.

▪ Actividad 2

Considerando que se desea desarrollar un sistema de información de gestión académica para una institución de educación media donde se realice matriculación, registro de notas, registro de asistencia y

cobro de pensiones, considere obtener los requisitos de seguridad que usted implementaría. Realice una comparación con algunos de sus compañeros y consulte con su tutor para tener una retroalimentación.

En esta semana se estudiará los conceptos de dos temas importantes que es la seguridad sobre aplicaciones Web y el tema del control de acceso en sistemas que es importante en los actuales momentos. Como nos identificamos frente a los sistemas es de importancia en el desarrollo de aplicaciones Web.



Semana 10

4.6. Seguridad en aplicaciones Web. OWASP

Se considera ya la seguridad de aplicaciones Web como una disciplina de la seguridad informática. En la actualidad los cambios que han implementado las organizaciones han implementado una mayor cantidad de aplicaciones Web para llegar a sus clientes, pasando de páginas estáticas o páginas dinámicas/transaccionales pensando siempre en que el cliente pueda conectarse desde diferentes sitios con una mayor disponibilidad es decir 24/7.

De la misma manera los problemas de seguridad van aumentando y ante cualquier defecto de los sistemas se explotan dichas vulnerabilidades por parte de hacker para causar afectaciones a los usuarios. El cambio ha sido muy significativo y también la aparición de nuevos lenguajes de programación con PHP, JavaScript, Python, Ruby, etc. Muchos framework de trabajo para el desarrollo de aplicaciones, aunque muchos de ellos incorporan temas de seguridad no se llega a completar los temas de construcción segura de aplicaciones.

OWASP, considerada como una organización sin fines de lucro nos presenta algunas recomendaciones para mejorar la seguridad del software. OWASP proporciona herramientas de software y documentación las mismas que están basadas en el conocimiento sobre la seguridad de las aplicaciones. Además, OWAS pone a disposición herramientas libres que se pueden encontrar en su sitio Web para que cualquier usuario acceda al uso de estas herramientas según la necesidad, es de esta forma que se recomienda revisar el sitio.

Cada 3 años OWASP publica su top 10 de los riesgos de seguridad más importantes que han sido clasificados y encontrados en diferentes sitios Web esto con la finalidad de ayudar a los programadores a considerar estos riesgos que se presentan para que sean corregidos y aplicados en las empresas o equipos de desarrollo de software.

A continuación, se mencionan los 10 problemas encontrados en la versión actual que es la 2017 (se está trabajando en la 2020).

- A1: 2017-Inyección
- A2: Autenticación rota en 2017
- A3: Exposición de datos confidenciales en 2017
- A4: Entidades externas XML 2017 (XXE)
- A5: 2017-Control de acceso roto
- A6: 2017-Configuración incorrecta de seguridad
- A7: 2017-Cross-Site Scripting XSS
- A8: Deserialización insegura de 2017
- A9: 2017: uso de componentes con vulnerabilidades conocidas
- A10: Registro y monitoreo

A continuación, se realizará una explicación de algunos de estos puntos:

- **Inyección de código:** este ataque inserta código fuente (SQL, SSI, HTML, etc.) al sitio Web atacado, cambiando su funcionalidad original o revelando datos que se encuentran almacenados en las bases de datos utilizadas.

SQL- Structured Query Language o Lenguaje de consultas estructuradas

SSI - Server Side Include) técnica de explotación de servidor, permite a un atacante sobre una aplicación Web enviar código

HTML - HyperText Markup Language o Lenguaje de Marcas de Hipertexto

- **Cross Site Scripting (XSS):** basado en la inserción de código o scripts en el sitio atacado, logrando que el visitante al ingresar al sitio lo ejecute y cumpla el cometido para el cual fue escrito, como robo de sesiones o datos vulnerables.

- **Fuerza bruta:** con la creación de procesos automatizados y generados al azar que mediante prueba y error logran conseguir el usuario y contraseña. Este tipo de ataque se puede dar en cualquier sitio que requiera autenticación para ingresar.
- **Denegación de servicios (DOS):** aprovecha de errores en la programación para lograr que el servidor utilice recursos como procesador y memoria, llegando al punto límite y haciendo colapsar el servidor Web por no dar más recursos. En consecuencia, se consigue sacar el sitio Web del aire.
- **Fuga de información:** más que ser un ataque es un error de administración del sitio, consiste en dejar público el registro de errores, facilitando la observación de fallas exactas del sistema, tomar provecho de estas y obtener el control parcial o total del sitio.

A continuación, le invito a profundizar su conocimiento sobre Seguridad en aplicaciones Web, OWASP.

4.6.1. Ataques sobre bases de datos - Inyección SQL

Debido a la gran flexibilidad con que cuenta el lenguaje SQL, la existencia de grandes bancos de información accesible a través de este lenguaje y la generación de nuevas y complejas formas de acceder de manera ilegal a la información privada, es que se torna imprescindible la aplicación de diferentes estrategias de seguridad que garanticen la estabilidad, accesibilidad, disponibilidad, privacidad, etc., de esta información.

En esta guía nos centraremos en el tipo de ataques conocido como *SQL Injection* o *Inyección SQL en español*, ya que a este según Venkatesh & Rami (2014), OWASP lo ha posicionado en la primera posición del Top 10 de vulnerabilidades de las aplicaciones Web en el año 2013.

Es un método de infiltración de código invasor que se vale de vulnerabilidades existentes en aplicaciones Web. Generalmente se da al momento de validar datos ingresados mediante formularios, una URL o cualquier otra forma de captura de información, que son evaluados por los servidores de bases de datos y por su estructura generan validaciones legítimas permitiéndonos el acceso para realizar operaciones en forma ilegal.

El origen de la vulnerabilidad radica generalmente en la inexperiencia de los desarrolladores, la no aplicación de suficientes restricciones a los parámetros de entrada, el incorrecto chequeo y/o filtrado de variables de ingreso de información utilizadas, la falta de control de privilegios de usuarios y la utilización de concatenación de strings principalmente.

Según Venkatesh & Rami (2014), entre los objetivos principales de las inyecciones SQL tenemos:

- Lectura de información sensible de la base de datos.
- Modificación de datos de la base de datos.
- Adquirir privilegios de administrador, ejecutar consultas administrativas y comandos de gestión de la base de datos, tales como el apagado de la misma.
- Recuperar el contenido de archivos o registros desde la base de datos.
- En algunos casos la ejecución de los comandos del sistema operativo.

Un ataque de Inyección SQL exitoso puede permitir al atacante interactuar con gran libertad sobre las bases de datos, dando autorización para leer, insertar, actualizar, eliminar datos y aún ejecutar distintos comandos SQL sobre esta. Operaciones que dependerán del tipo de autorización o de los permisos que se tenga en las bases de datos y dependiendo de la experticia del atacante ejecutar comandos del sistema operativo e iniciar otro tipo de ataques en el servidor. La magnitud o gravedad de estos ataques dependerá también de la aplicación a la cual se accede y de los datos contenidos en ella.

Inyección de SQL es en realidad uno de los tipos de ataques más comunes en lo referente a vulnerabilidades Web que pueden ocurrir en cualquier lenguaje de programación, esto es debido a la alta flexibilidad prestada por el lenguaje SQL. Mientras más poder otorguen los sistemas de gestión de bases de datos a los desarrolladores, se dará más oportunidad a los atacantes para cambiar el aspecto de los ataques y evitar los comunes sistemas de detección.

4.6.2. Inyección SQL sobre bases de datos relacionales

Se pueden considerar algunos mecanismos de ataques entre los que se pueden mencionar los mecanismos de primer orden los que tendrían un efecto directo sobre el sistema y los mecanismos de segundo orden que son aquellos en los que no existe efecto directo.

Nos centraremos en los ataques de primer orden, los cuales según sus mecanismos ya sean de ingreso a la base de datos como de medio de recibir respuesta desde esta, han sido clasificadas con diferentes nombres por algunos. En esta guía adoptaremos los términos más difundidos o mejor conocidos.

- a. **Mecanismos de Ataques de Inyección SQL.** Por su mecanismo de ataques de Inyección tenemos:

- **Inyecciones a través de entradas de usuario.** Este tipo de ataque, se inyecta comandos SQL por medio de las entradas adecuadamente diseñadas para los usuarios.
- **A través de cookies.** Estos pequeños archivos que se almacenan localmente en la máquina cliente son generados por las aplicaciones Web y contienen información de estado. Son utilizados por las aplicaciones Web para restaurar la información del cliente y pueden ser un medio para enviar consultas SQL que vulneren o envíen un ataque a la aplicación.
- **A través de variables de servidor.** Este ataque se vale de las colecciones de variables que contienen el protocolo HTTP y que son enviadas a través de la línea de navegación. Los atacantes podrían falsificar los valores colocados en ellas para la generación de consultas.

Así mismo, por la forma en como el cliente recibe las respuestas desde las aplicaciones o bases de datos atacadas se han clasificado como:

- **Inband (en la banda):** Es el método más simple, la información extraída se muestra en el mismo canal utilizado para realizar el ataque. Por ejemplo, mostrar una lista de datos extraídos desde la base en la página actual.

- ***Out-of-band (fuera de banda)***: Se utiliza un medio alternativo como el correo electrónico u otro para recibir la información extraída.
 - ***Inferential (inferencial)***: En la cual el atacante no recibe ninguna información, pero puede ver los resultados de sus ataques analizando el comportamiento de las aplicaciones.
- b. **Tipos de Ataques de Inyección SQL**. Entre los principales tipos de ataques tenemos:

Tautologías. (Tautologies). La intención de este tipo de ataque es la de pasar por alto cualquier tipo de autenticación de usuario inyectando una o más sentencias condicionales que permitan que una validación de siempre una respuesta sintácticamente verdadera, permitiendo así el acceso a datos no autorizados.

Los ataques de SQL más comunes son aquellos que se realizan en acceso de aplicación al momento de validar los usuarios o contraseñas o a través de un formulario, en el cual se usan los siguientes métodos: Ver ejemplos de los ataques SQL.

Ejemplos de los ataques SQL

Existen muchos recursos en la Web. Puede revisar este [ejemplo](#) para profundizar en el tema, de igual manera en el sitio Web [OWASP Cheat Sheet Series](#) podrá encontrar estos temas con mayor profundidad.

4.6.3. Inyección sobre Bases de Datos NoSQL

En estas bases de datos NoSQL *Not Only SQL*, debemos priorizar algunas propiedades a costa del debilitamiento de otras según los requerimientos de la aplicación, considerando una nueva tripleta de requisitos que incluyen: consistencia (C), disponibilidad (A) y tolerancia a la partición (P).

Para nuestro estudio nos centraremos en el sistema de base de datos NoSQL orientado a documentos *MongoDB*, el cual actualmente está siendo utilizado por algunas compañías como Google, Facebook, Foursquare, eBay, etc. Además, la orientación a documentos sobre el cual se organizan sus contenidos es diferente a la organización de tablas utilizado por el modelo relacional, lo que nos permite evaluar las similitudes de vulnerabilidades entre dos sistemas no tan similares.

Estas bases de datos no se construyen a base de tablas y no utilizan el lenguaje de consulta SQL, pero ¿Significa esto que no son vulnerables a ataques de SQL Injection?

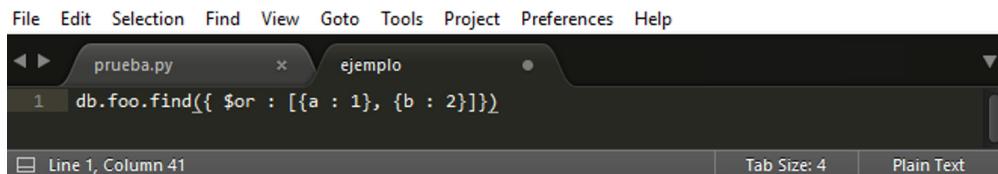
Pues como podemos observar en la conferencia Palanco, 2011, existen algunos tipos de inyecciones NoSQL que pueden ser utilizadas para vulnerar bases de tipo MongoDB, para su análisis lo hemos clasificado en tres importantes grupos:

JSON Injection. De la misma manera como se utiliza SQL para construir consultas y hacer peticiones a una base de datos relacional en base a parámetros dados por el usuario, también podemos crear peticiones a bases NoSQL con JSON, por lo tanto, también existe la vulnerabilidad manipulando estas peticiones para obtener respuestas no permitidas desde la base de datos.

Consideremos la consulta tomada de Erlend (2010).

Figura 41.
Sentencia de ejecución

Ejemplo: 05



The screenshot shows a code editor window with a menu bar at the top. The menu items are: File, Edit, Selection, Find, View, Goto, Tools, Project, Preferences, and Help. Below the menu, there are two tabs: "prueba.py" and "ejemplo". The "prueba.py" tab is active, showing the following code in its editor area:

```
1 db.foo.find({ $or : [{a : 1}, {b : 2}]}))
```

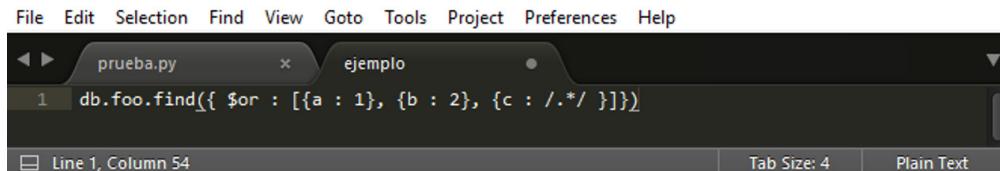
At the bottom of the editor, there is a status bar with the text "Line 1, Column 41" on the left, "Tab Size: 4" in the middle, and "Plain Text" on the right.

En la cual se solicita realizar una búsqueda en la base de datos foo, mediante una condicional OR.

Suponiendo que el número 2 en la consulta anterior viene de concatenación de una cadena de entrada o de la lectura de una cadena de entrada digitada por un usuario, se podría manipular tal cadena para obtener una inyección como la siguiente:

Figura 42.

Ejecución de sentencias



The screenshot shows a code editor window with a menu bar at the top. The menu items are: File, Edit, Selection, Find, View, Goto, Tools, Project, Preferences, Help. Below the menu, there are two tabs: "prueba.py" and "ejemplo". The "prueba.py" tab is active and contains the following Python code:
```python  
1 db.foo.find({ \$or : [{a : 1}, {b : 2}, {c : '/.\*/' }]}))  
```  
At the bottom of the editor, it says "Line 1, Column 54". To the right of the editor, there are buttons for "Tab Size: 4" and "Plain Text".

Lo que permitiría obtener una respuesta *True* en cualquier caso.



Para una mejor comprensión de tema, realice la *Actividad 1* que se presenta al final de esta semana.

4.7. Protección de sitios con protocolo HTTPS

Es importante que nuestros sitios que ocupan el protocolo de transferencia de hipertexto HTTP sea seguro, o sea que utilicemos HTTPS, ya que es un protocolo que protege la integridad y la confidencialidad de los datos que interactúan entre los usuarios y el sitio Web.

Sabemos que actualmente la información que está a disposición de los usuarios y los programas de concientización van orientando a que las personas se fijen en los sitios donde accede, donde van a realizar sus compras o donde van a colocar algún dato, el usuario quiere que su información sea privada y segura, entonces al ver si un sitio no está utilizando este protocolo puede desistir de ingresar y si es una empresa comercial podría perder un posible cliente.

Con la utilización del protocolo HTTP el envío de informaciones proporciona tres características fundamentales:

- **Autentificación:** proporciona protección ante posibles ataques de intermediarios, demostrando que usuarios registrados se comunican son nuestro sitio Web.
- **Integridad:** ya que los datos no puedan dañarse ni modificar durante el proceso de trasferencia de ningún modo o sea de forma intencionada o cualquier otro modo sin que sea de alguna forma se detecte.

- **Cifrado:** que corresponde al proceso de ocultar la información original cambiando o aplicando algún método de encriptación, es así que mediante este protocolo los datos que se intercambian entre las entidades que están comunicándose se mantienen a salvo, no permitiendo que se pueda interceptar el flujo de trabajo que se está realizando. Es importante conocer también que mediante este protocolo no se puede determinar desde fuera sobre qué páginas se está interactuando dentro de nuestro sitio.

Para la implementación de este protocolo en nuestros sitios es necesario realizar algunas acciones, que se pueden encontrar en (Google, 2021).

4.8. Uso de certificado SSL

Un certificado SSL es un archivo de datos que relaciona digitalmente una clave criptográfica con los datos de una organización. Una vez instalado en el servidor Web, el certificado activa el candado y el protocolo https y de esta forma se habilita una conexión segura desde el servidor Web hasta el navegador. Normalmente, el SSL se utiliza para proteger las transacciones con tarjeta de crédito, la transferencia de datos y los inicios de sesión y más recientemente se está convirtiendo en el estándar para proteger la navegación por redes sociales.

El uso de certificados SSL en un portal Web ofrece un gran número de ventajas.

- Mejora la seguridad: su uso, garantiza que toda la información que se mueva entre el ordenador del usuario y portal esté encriptada.
- Legitimación del sitio Web: se consigue que una entidad independiente dé el visto bueno al sitio Web.
- No da problemas: su uso es compatible con el 99% de los navegadores existentes en el mercado.

Antes de comprar o implementar un certificado SSL se debe considerar lo siguiente:

- Los certificados SSL son una especie de pasaporte digital que contiene, entre otros, el nombre del titular, un número de serie que lo identifica y la firma digital de la autoridad emisora.

- Los certificados digitales no solo verifican la identidad de una página Web, sino que además cifran la información que se envía y se recibe utilizando el protocolo de seguridad Secure Sockets Layer (capa de puertos seguros). Evitando que los cibercriminales roben la información delicada.

La adquisición de un certificado SSL para el sitio es rápido y sencillo. En primer lugar, hay que comprar el certificado SSL de elección en cualquier proveedor. A continuación, se deberá introducir los datos (que la autoridad de certificación verificará) y una vez emitido, se tendrá que instalarlo desde el panel de control del servidor.

¿Cómo funciona el Certificado SSL?

Al escribir en la barra de direcciones de un navegador la URL utilizando el protocolo HTTPS, por ejemplo, <https://www.abc.com>, esta petición, el navegador envía un mensaje al sitio de destino indicando que quiere establecer conexión segura, a la vez que le envía información sobre la versión del protocolo SSL que soporta y otros parámetros de interés para llevar a cabo la conexión. Con base en la información enviada por el navegador, el servidor Web de destino responde con un mensaje informando que está de acuerdo con establecer una conexión segura con los datos suministrados, una vez que ambos conocen los parámetros de conexión, el sitio de destino presenta su certificado de seguridad para presentarse como un sitio confiable.

A continuación, la figura 43 se muestra la conexión segura con Certificado SSL.

Figura 43.
Esquema de implementación certificado SSL





Para una mejor comprensión de este tema, realice la *Actividad 2* donde se aplicará los conceptos tratados en este apartado.

4.9. Control de Acceso

Todas las aplicaciones que deben ser realizadas deben implementar una forma de controlar el acceso al mismo. El control de acceso se basa en tres factores: algo que sabes, algo que eres y algo que tienes. Veamos:

Algo que sabes, este proceso se puede conseguir con la implementación de usuario, *password* y preguntas de verificación. Algunas personas usan las mismas contraseñas en varias cuentas, es por eso por lo que cuando hay la debilidad sobre alguna aplicación y los claves son conseguidas la exposición de las otras aplicaciones queda también en riesgo.

Algo que eres, se incluyen el uso de huellas digitales, métodos de autenticación mediante herramientas biométricas, reconocimiento de voz, reconocimiento de iris. En la actualidad los computadores personales ya incorporan lectores de huellas digitales o de la misma manera la mayoría de los teléfonos actuales poseen ya estas características. Aunque esto no es del 100% seguro, se han registrado casos que las personas muy parecidas, madre e hija, le han permitido desbloquear el teléfono con un reconocimiento del rostro.

Algo que tienes, este factor en la actualidad es uno de los más usados, ya sea con la utilización de claves externas para verificación como es la utilización de una USB, otra versión es complementar con el uso de códigos de verificación luego de pasar una primera conexión donde es necesario ingresar el código de verificación que llega ya sea a un correo electrónico o al dispositivo personal como un celular.

En la actualidad el doble factor de identificación como es conocido ha sido implementado en la mayoría de las aplicaciones, ya algunas aplicaciones tradicionales sociales están implementando una obligatoriedad en las mismas, como preguntas, mensajes al mail y mensajes al celular.

A continuación, vamos a mirar un ejemplo donde se colocan factores de doble identificación de una institución financiera de la localidad, donde para la página web se utiliza de una forma el doble factor de acceso, que realmente pasa hacer como tener 3 factores:

A. Acceso a la banca virtual a través de la página web

1. Control de acceso inicial, se realiza mediante comprobación de usuario y una contraseña previamente registrada, figura 44.

Figura 44.

Ingreso al sitio a través de usuario y clave

Usuario

Clave

Ingresar

[¿Olvidó su clave? / Desbloqueo](#)

[Activar Banca Electrónica](#)

[Abre tu cuenta en línea aquí](#)

Nota. Captura de pantalla sitio web.

2. Se implementan dos mecanismos de acceso adicionales: el primero es responder a una pregunta que está registrada y el segundo se debe seleccionar una imagen previamente registrada, figura 45.

Figura 45.

Pantalla de ingreso de factores de verificación: respuesta a pregunta y selección de imagen

ACCESO BANCA ELECTRÓNICA

Bienvenido DANILO JARAMILLO HURTADO:

Por favor responda la siguiente pregunta y seleccione una imagen.

Pregunta de seguridad: Respuesta:

¿Marca de auto favorita?: Cambiar Pregunta

Por favor seleccione la imagen que asoció al proceso de registro/actualización de información y presione el botón ACEPTAR para continuar.

CANDADO PLAYO ESFERO GAFAS CONO

BICICLETA TECLA MICROFONO CORBATA IMPRESORA

Ingresar

Nota. Captura de pantalla de sitio web.

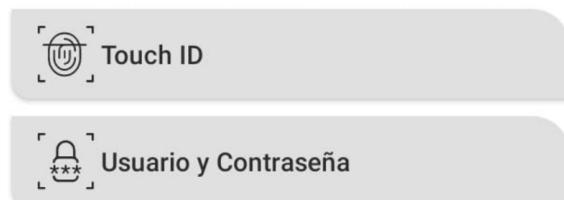
B. Acceso a la banca virtual a través del móvil

1. En el caso de esta aplicación para el control de acceso se pueden seleccionar dos alternativas. Se ingresará utilizando el usuario y contraseña o la utilización del lector biométrico del teléfono, figura 46.

Figura 46.

Pantalla para ingreso desde aplicación móvil

Elige el modo de ingreso



Nota. Captura de pantalla aplicación web.

2. En el caso de haber seleccionado la opción de usuario y contraseña se debe ingresar primero el usuario, figura 47.

Figura 47.

Pantalla de ingreso validando únicamente usuario

La captura de pantalla muestra una interfaz de usuario para el 'Ingreso de Usuario'. En la parte superior, hay un encabezado verde con la etiqueta 'Ingreso de Usuario' y un icono de flecha hacia la izquierda. Abajo de este, en el fondo blanco, se encuentra un cuadro de texto que dice: 'Por favor ingresa tu nombre de usuario'. Debajo de este cuadro, se ve la palabra 'Usuario' seguida de un cuadro vacío para la inserción de texto.

Nota. Captura de pantalla aplicación web.

3. Posteriormente el Ingreso de la contraseña y seleccionar la imagen, para este caso no se utiliza el factor de pregunta y respuesta.

Figura 48.

Pantalla de ingreso validando contraseña y selección de imagen

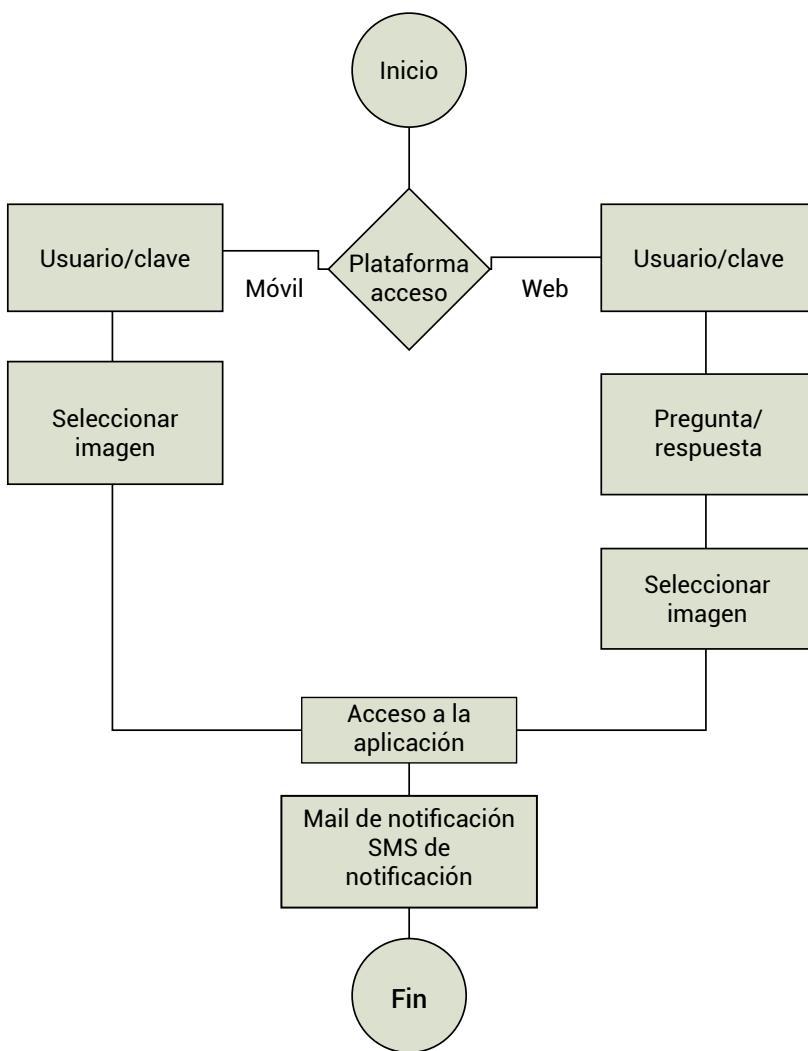


Nota. Captura de pantalla aplicación web.

Como se ve hay una variación de implementación de varios factores de seguridad para acceso a estas aplicaciones. A continuación, trataremos de realizar un diagrama analizando estos dos casos, figura 49.

Figura 49.

Flujo de análisis de acceso a la aplicación tanto web como móvil



Como vemos, este diagrama presenta la secuencia ideal de acceso. ¿Cómo podría modificar el diagrama para controlar en el caso que no se cumpla con la validación?



Hemos terminado esta unidad, estos temas son muy interesantes ¿Cómo le fue con su comprensión? Existió algunos temas que le resultaron familiares, es importante profundizar en aquellos temas que no han quedado claro. No dude en escribir a su profesor tutor por los diferentes medios de comunicación. Ayúdese de las tutorías para despejar sus dudas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

- Revise el sitio [OWASP](#) realice un recorrido por el mismo revise su TOPTEN, revise la guía de prueba de seguridad móvil de OWASP.
- Se colocará el artículo métodos y herramientas para el análisis forense de dispositivos móviles, para su lectura, además en el mismo podrá encontrar bibliografía que le servirá para comprender mejor este tema.

▪ **Actividad 1**

Revise el siguiente video, [Webinar Gratuito: Inyección SQL](#), realice el proceso de verificación de inyección SQL de un sitio, replicando el ejemplo del video planteado por el autor.

▪ **Actividad 2**

En el entorno virtual de aprendizaje encontrará un manual para realizar implementación de un certificado SSL, con el mismo impleméntelo en un sistema Web que usted tenga. Se colocará también un archivo .zip con un proyecto para poder realizar la implementación en el caso de que usted no tenga un proyecto

Una vez que ha estudiado los conceptos relacionados con la Unidad 4, le invito a desarrollar la autoevaluación con el fin de evaluar los conocimientos adquiridos hasta el momento. Posterior a eso usted podrá encontrar al final de este Texto Guía la solución a cada una de las preguntas.

¡Éxitos en la autoevaluación!



Autoevaluación 4



Una vez que ha estudiado los conceptos relacionados a la unidad 4, le invito a desarrollar la autoevaluación con el fin de evaluar los conocimientos adquiridos hasta el momento. Posterior a eso, usted podrá encontrar al final de este texto-guía la solución a cada una de las preguntas.

¡Éxitos en la autoevaluación!

- 1. ¿Cuál de los siguientes requisitos para un sistema de gestión académica se puede referir como un requerimiento no funcional?**
 - a. Se debe actualizar la ficha del estudiante antes de cada matrícula.
 - b. No se debe permitir que dos usuarios con el mismo nombre estén en el sistema al mismo tiempo.
 - c. Los estudiantes podrán consultar sus notas.
- 2. ¿Cuál de estos principios pertenece al diseño seguro?**
 - a. Acceso a los sistemas.
 - b. Basados en password.
 - c. No dejar procesos de seguridad a nivel de usuario final.
- 3. ¿Cuál se puede considerar un requisito de seguridad?**
 - a. Doble factor de identificación.
 - b. Hace lo más simple las cosas.
 - c. Implementar la seguridad en todas las capas.
- 4. ¿Cuál es una herramienta de revisión de código?**
 - a. Sonarqube.
 - b. Autopsy.
 - c. MobilEdit.

5. OWASP, cada qué tiempo saca la nueva versión:

- a. Cuatro.
- b. Tres.
- c. Cinco.

6. “Aprovecha de errores en la programación para lograr que el servidor utilice recursos como procesador y memoria, llegando al punto límite del mismo”:

- a. XSS.
- b. SQL-i.
- c. DoS.

7. Lector de huella biométrica:

- a. Algo que sabes.
- b. Algo que eres.
- c. Algo que tienes.

8. Pin de verificación:

- a. Algo que sabes.
- b. Algo que eres.
- c. Algo que tienes.

9. Pregunta secreta:

- a. Algo que sabes.
- b. Algo que eres.
- c. Algo que tienes.

10. Medir en lo posible las fugas de datos, tomando en consideración el riesgo en la protección de datos” hace referencia a:

- a. Pruebas de penetración.
- b. Arquitectura de análisis de riesgos.
- c. Revisión de código.

Puede verificar las respuestas de esta autoevaluación al final del Texto Guía.

[Ir al solucionario](#)

Si su puntaje no es bueno, es importante que vuelva a revisar los contenidos de la unidad y los recursos de aprendizaje, no olvide que puede interactuar con su tutor por cualquier medio de comunicación que brinda la UTPL para que aclare sus inquietudes.

Resultado de aprendizaje 8

- Describir la importancia de elementos clave que participan en el seguimiento de incidentes para desarrollar un proceso de manejo y reporte de incidentes a través de un plan de manejo de incidentes.

Contenidos, recursos y actividades de aprendizaje



Semana 11

Unidad 5. Análisis forense

En la actualidad se presentan en los diferentes medios de comunicación casos delincuenciales donde se ha llegado a determinar la participación de personas por la manipulación que se ha realizado en dispositivos electrónicos que manejan, ya sea la intercepción de llamadas telefónica, mensajes de texto entre los actores, correos electrónicos que se envían entre sí, grabaciones de cámaras digitales, etc. Muchas de las veces las personas involucradas realizan una eliminación de estos archivos pensando que los mismos han desaparecido de los dispositivos, que luego han podido ser recuperados.

Existe también el manejo de redes sociales desde donde se publican *post*, acceso a sitios no autorizados o no adecuados, estas evidencias digitales siempre dejarán un rastro que puede ser encontrado por un perito informático con la ayuda de herramientas, este trabajo es conocido como un análisis forense informático. Este tema es muy interesante vamos a adentrarnos en el mismo.

¡Éxitos en el estudio de esta unidad!

5.1. Análisis forense informático

El análisis forense parte de dar una respuesta a las siguientes interrogantes: ¿De qué se trata? ¿Para qué sirve? ¿Qué técnicas y herramientas se deben

usar? ¿Cuál es el procedimiento para seguir? ¿Qué leyes, de acuerdo al código vigente en el país se aplican mediante un delito informático?

Vamos a adentrarnos a un nuevo tema. Es importante que tenga a la mano su material de trabajo, así como es importante también conocer que existen informáticos forenses que están buscando nuestra información para atacar nuestros sitios o acceder a nuestros sistemas. A continuación, revise la siguiente infografía que le podrá ayudar a entender este tema: [Cómo disminuir tu rastro en internet](#).

5.2. ¿Qué es y para qué sirve el análisis forense informático?

Para iniciar el estudio de este capítulo vamos a revisar algunos conceptos que han sido propuestos por varios autores sobre el análisis forense:

En (Cajo et al., 2018) se menciona que el análisis forense Informático el análisis forense informático, en un sentido formal, es definido como “un conjunto de principios y técnicas que comprende el proceso de adquisición, conservación, documentación, análisis y presentación de evidencias digitales y que llegado el caso puedan ser aceptadas legalmente en un proceso judicial”.

Para (Herrera et al., 2019) “La Informática Forense es una disciplina de las ciencias forenses que involucra la aplicación de metodologías científicas para identificar, preservar, recuperar, extraer, documentar e interpretar evidencias procedentes de fuentes digitales con el fin de facilitar la reconstrucción de los hechos, para usar luego dichas evidencias como elemento probatorio en un proceso judicial”.

Basándose en los conceptos anteriores se puede definir al análisis forense informático como *un proceso y/o metodología que tiene la finalidad de probar y reconstruir un hecho o suceso, a través de las pruebas realizadas en un laboratorio*.

¿Para qué sirve el análisis forense?

El análisis forense informático permite la aplicación de técnicas y herramientas para la reconstrucción de pruebas a ser usadas, para la argumentación científica ante un delito e incidente.

Hay que considerar que cuando un usuario no autorizado toma el control de un sistema, el mismo puede instalar diferentes aplicaciones o puertas traseras que en lo posterior le permitirán entrar al sistema. Muchas de las veces el acceso seguirá, aun cuando se corrija la vulnerabilidad original que le permitió el control del sistema. Pues muchas de las veces no se eliminan totalmente la modificación realizada. Será labor del análisis forense conocer que acciones realizó el atacante en el sistema para detectar este tipo de actividades.

Para una mejor comprensión de este tema, realice la *actividad 1* de las actividades de aprendizaje recomendadas.

5.3. Tipo de análisis forense

Los tipos de análisis forense que se mencionan en (Jaramillo & Guamán, 2017) y dependen del punto de vista del que se va a analizar, entre ellos tenemos:

- a. **De sistemas:** en el mismo se tratan los incidentes de seguridad en servidores, computadores de trabajo con los sistemas operativos como MAC OS, Windows, UNIX y sistemas GNU/Linux.
- b. **De redes:** engloba el análisis de diversas redes de computadores (cableadas, wireless, bluetooth, etc.).
- c. **De sistemas embebidos:** se analizan incidentes presentados en dispositivos como teléfonos, tabletas, PDA, etc., ya que un sistema embebido posee una arquitectura semejante a la de un computador personal.

5.4. Principios del análisis forense

Al comenzar un examen forense existen un sin número de elementos básicos que se deben tomar en consideración en cada una de las fases tales como:

- a. **Evitar la contaminación:** se debe evitar la incorrecta manipulación de la evidencia, pues evitar una incorrecta interpretación o análisis, esto se presenta en muchas ocasiones por la premura de realizar las

cosas, muchas veces se cree que el personal de TI sabe de todo y al realizar una manipulación rápida sin considerar lo que puede afectar el dispositivo en lo posterior puede no considerarse como una prueba en un proceso legal.

- b. *Actuar metódicamente*: el investigador debe ser el custodio de su propio proceso, así, cada uno de los pasos realizados, las herramientas utilizadas, los resultados obtenidos deben estar bien documentados estableciendo responsables, fechas, horas, actividades, es así que ante un problema si no se tiene el conocimiento se debe llamar o asesorarse de expertos.
- c. *Controlar la cadena custodia*: responder a una diligencia y formalidad especial para documentar cada uno de los eventos que se han realizado con la evidencia, aquí se debe evitar la manipulación y seguir los pasos que recomiendan las diferentes metodologías de análisis forense.

Como estudiante de la carrera de tecnologías de la información debe tener claro que estos temas son importantes para quienes son parte del departamento de TI, por lo que se recomienda tomar apuntes e ir desarrollando las actividades. Además, contactar a su profesor tutor por cualquier duda que tuviera.

Algo importante en este tema, como se lo mencionó, debemos dejar de pensar que como parte del departamento de TI o informática como lo llamen en las empresas podemos y es una obligación hacer o saber de todo el ámbito de informática, muchas de las veces es preferible que usted solicite la ayuda de un experto si el problema es grave y puede tener implicaciones legales, pues la evidencia como se ha mencionado podría dejar de ser de utilidad si usted realiza una mala manipulación. Recuerde cuando exista un problema que puede llevar a un problema más grave recordar estos principios.

5.5. Usos de la informática forense

En (Jaramillo & Guamán, 2017), se mencionan que existen varios usos de la Informática Forense, provenientes de la vida diaria y no necesariamente están relacionados con la informática forense, tales como:

- a. **Persecución criminal:** evidencia incriminatoria para procesar en crímenes como homicidios, fraude financiero, tráfico y venta de drogas, evasión de impuestos o pornografía infantil.
- b. **Litigación civil:** casos que tratan con fraude, discriminación, acoso y/o divorcio.
- c. **Investigación de seguros:** la evidencia encontrada en computadoras puede ayudar a las compañías de seguros a disminuir los costos de los reclamos por accidentes y compensaciones.
- d. **Temas corporativos:** acoso sexual, robo, mal uso o usurpación de información confidencial o propietaria, o espionaje industrial.
- e. **Mantenimiento de la ley:** búsqueda inicial de órdenes judiciales, como la búsqueda de información una vez se tenga la orden judicial para realizar una búsqueda exhaustiva.

5.6. Uso de análisis forense

El objetivo principal de un investigador forense es identificar a todos los sistemas controlados por el intruso, comprender los métodos utilizados para acceder a estos sistemas, los objetivos del intruso y la actividad que ha desempeñado durante su estancia dentro del sistema comprometido.

La información obtenida tiene que ser compartida con el resto de los miembros del equipo forense, a fin de evitar la pérdida de información. También el objetivo del investigador es la protección del estado de sitio contra modificaciones para evitar pérdidas de información o pruebas.

Cada sistema operativo es un entorno ideal en el cual realizar tareas de análisis forense pues está dotado de gran variedad de herramientas que facilitan todas las etapas que se deben llevar a cabo en la realización de un análisis exhaustivo de un sistema comprometido.

El sistema Linux presenta algunas características que le dotan de grandes ventajas a la hora de ser utilizado como herramienta de análisis forense de sistemas. Estas características son:

- Todo, incluido el *hardware* se trata y representa como un fichero.

- Soporta numerosos tipos de sistemas de archivos, muchos no reconocidos por Windows.
- Permite montar los sistemas de archivos.
- Permite analizar un sistema en funcionamiento de forma segura y poco invasiva, dirigir la salida de un comando a la entrada de otros (múltiples comandos en una línea).
- Permite revisar el código fuente de la mayoría de sus utilidades y generar dispositivos de arranque.

Existen algunas herramientas en la Web que por ejemplo nos permiten extraer metadatos de un archivo para poder determinar que se realizó con el mismo. Una de estas herramientas es FOCA, en la página [CIBERPATRULLA](#) nos presenta un ejemplo de la aplicabilidad de esta herramienta, sería importante que realice esta pequeña práctica.

5.7. Manejo de incidentes informáticos

Según la norma ISO 27035, un incidente de seguridad de la información es indicado por un único o una serie de eventos de seguridad de la información indeseada o inesperada, que tienen una probabilidad significativa de comprometer las operaciones de negocio y de amenazar la seguridad de la información.

También se considera a un incidente informático como una violación o intento de violación de la política de seguridad, de la política de uso adecuado o de las buenas prácticas de utilización de los sistemas informáticos.

A nivel jurídico se dice que los peritos informáticos se enfrentan a una variedad de casos reales, entre los que se mencionan:

- Realizar copias sin autorización de archivos de la empresa.
- Acoso a personas a través de redes sociales, correo electrónico o SMS, envío de spam, posesión de pornografía infantil.
- Difusión de información reservada como cuentas bancarias, montos de remuneraciones de los empleados, robo de datos bancarios.

- Ataques a sistemas informáticos, tanto internos de la empresa como externos a personas u organismos utilizando medios internos como equipos y red, instalación de *keylogger* para robar información.
- Copia o difusión de libros en formato digital, de música, de vídeos, o sea referente a la propiedad intelectual etc.
- Estafas, fraudes, alteración de precios, ofertas internas para beneficio propio.
- Edición, divulgación, acceso o posesión de pornografía ilegal, como, por ejemplo, la pornografía infantil.
- Inyección de programas infecciosos, como virus y gusanos, dentro de sistemas informáticos.
- Destrucción de hardware o alteración de datos, así como instalación y uso de programas ocultos como son los caballos de Troya, *backdoors*, *rootkits*, etc.

¿Cómo le pareció el tema? A partir de estos elementos, realice la *actividad 1* dentro de las actividades de aprendizaje recomendadas.

Para el manejo de los *incidentes informáticos*, al igual que en el análisis forense se requiere de un procedimiento que determine la respuesta inmediata ante el incidente o suceso. Ver recurso interactivo.

Fases para el manejo de incidentes informáticos

Finalmente, una actividad que debe realizarse, al margen del manejo de incidentes, es la ejecución de una auditoría de planes de respuesta a incidentes que evalúe por lo menos los siguientes aspectos:

- **Políticas y procedimientos de respuesta a incidentes**
 - Herramientas y recursos.
 - Modelo y estructura del equipo.
 - Entrenamiento y capacitación del personal; y,
 - Documentación de incidentes y reportes. La evaluación de los elementos anteriores permitirá identificar deficiencias y

problemas en relación con las políticas, regulaciones y mejores prácticas requeridas por el equipo de respuesta a incidentes.

Por lo tanto, una vez identificado el incidente y la gravedad de este, se da paso al análisis forense informático como tal, el cual determinará cómo fue vulnerado el sistema, cuándo, quién y qué hizo el intruso en el mismo.

Hemos terminado esta semana de trabajo, estos temas son muy interesantes ¿Cómo le fue con su comprensión? Existió algunos temas que le resultaron familiares, es importante profundizar en aquellos temas que no han quedado claro.



No dude en escribir a su profesor tutor por los diferentes medios de comunicación. Ayúdese de las tutorías para despejar sus dudas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

- Revise el sitio www.owasp.org, realice un recorrido por el mismo revise su TOPTEN, revise la guía de prueba de seguridad móvil de OWASP.
- Se colocará el artículo métodos y herramientas para el análisis forense de dispositivos móviles, para su lectura, además en el mismo podrá encontrar bibliografía que le servirá para comprender mejor este tema.
- En este [artículo](#) hay un aporte importante sobre el tema de análisis forense por lo que lo invito a revisarlo.

▪ Actividad 1

Busque en la red diferentes aspectos donde se hayan realizado procesos utilizando análisis forense informáticos sobre los temas que se tratan en este apartado. Use la siguiente tabla de ejemplo:

Tabla 25.

Ejemplo

Persecución criminal	Enlace web	Desaparición de una persona en España, el seguimiento se da por los mensajes eliminados en su celular.
Dentro de los en una de la fase final:		
Litigación civil:		
Investigación de seguros:		
Temas corporativos:		
Mantenimiento de la ley		

Nota. Copie la tabla en Word para llenar.

■ Actividad 2

Por cada uno de los casos reales que enfrentan los peritos que se mencionaron en el apartado anterior busque ejemplos en la Web donde se haya trabajado, por ejemplo:

- Publicidad engañosa o correo electrónico *spam*

Este [artículo](#) habla sobre la campaña de *spam Hacker who cracked your email and device Email Scam*

Se ha realizado en la semana anterior la definición de los conceptos, los tipos de análisis forense, así como los problemas con los que nos podemos encontrar al momento de realizar el análisis forense, en esta semana nos vamos a orientar al proceso en sí, primero conociendo una metodología y posterior conocer las herramientas y características de estas.



Semana 12

5.8. Metodologías de análisis forenses

En esta sección se considera algunas metodologías o *frameworks* que ayudan al análisis forense. Estas metodologías se pueden conseguir en la Web. En la presente guía se trata de dar una explicación general de las mismas, pero debe buscar las mismas y descargarlas, la mayoría de estas son gratis

5.8.1. Open Android Security Assessment Methodology OASAM

OASAM, es el acrónimo de Open Android Security Assessment Methodology es un framework de referencia de análisis de vulnerabilidades en aplicaciones Android, en la que el autor (DragonJar, 2021) señala que tiene por objetivo ser una metodología de análisis de seguridad de aplicaciones Android.

El autor establece los siguientes controles de seguridad:

- OASAM-INFO Information Gathering (): en esta fase se define la superficie de ataque.
- OASAM-CONF Configuration and Deploy Management (Análisis de la configuración e implantación): en esta fase se definen diferentes errores de configuración en las opciones de despliegue de las aplicaciones.
- OASAM-AUTH Authentication (Análisis de la autenticación): en esta sección se comprueban las funcionalidades relativas al uso de *logins* a través de la aplicación. Es importante recalcar que lo que se buscarán son vulnerabilidades en la aplicación Android, si la autenticación se realiza contra un tercero (WebService, servicio REST, etc.) la seguridad del tercero no será evaluada, solo las debilidades ligadas a la propia aplicación Android.
- OASAM-CRYPT Cryptography (Análisis del uso de criptografía): en la sección de autenticación se comprobarán las funcionalidades relativas al uso de la criptografía en el aplicativo. Esto puede ser al transmitir información o al almacenarla.
- OASAM-LEAK Information Leak (Análisis de fugas de información sensible): en la sección de autenticación se comprobarán las fugas de información a diferentes medios. La información sensible puede ser relativa al usuario o del propio teléfono.
- OASAM-DV Data Validation (Análisis de gestión de la entrada de usuario): en esta categoría se incluirán vulnerabilidades que tienen que ver con el manejo por parte de la aplicación de la entrada recibida por parte del usuario. La mala validación de la entrada del usuario es uno de los principales vectores de ataque, ya que puede permitir a un atacante alterar los flujos de información de la aplicación, inyectando

código y afectando gravemente a la aplicación y a los datos que ella contiene. En el *top ten* de riesgos en aplicaciones móviles, esta categoría constituye el puesto 4, denominándose *Client Side Injection*.

- OASAM-IS IDentro Cual nCtent Spoofing (Análisis de la gestión en la recepción de Intents): representa vulnerabilidades que tienen que ver con el envío de *intents* arbitrarios a un componente que espera recibir otro tipo de *intents*. De esta manera el atacante utilizará los filtros de la víctima para enviar datos que la víctima no espera y aprovecharse así de sus funcionalidades.
- OASAM-UIR Unauthorized Intent Receipt (Análisis de la resolución de *intents*): representa vulnerabilidades que tienen que ver con la resolución del envío de *Intents* implícitos. Cuando una aplicación envía un *Intent* implícito, no hay garantía de que una aplicación maliciosa no vaya a recoger dicho *Intent*, ya que una aplicación maliciosa podría registrar un *Intent Filter* que fuera capaz de pasar la resolución (*action*, *data* y *category*), a no ser que dicho *Intent* tenga requeridos una serie de permisos que la aplicación maliciosa no posea.
- OASAM-BL Business Logic (Análisis de la lógica de negocio la aplicación): En esta categoría se incluirán vulnerabilidades que tienen una componente más centrada en el propio diseño que la codificación. Los ataques sobre la lógica de negocio de una aplicación son peligrosos, difíciles de detectar y específicos a la aplicación.

5.8.2. Metodología Forense del Instituto Nacional de Estándares de Tecnología (NIST)

La guía (Ayers et al., 2014) ofrece información básica sobre la conservación, adquisición, exploración, análisis y presentación de informes de las pruebas digitales en los teléfonos celulares, pertinentes para la aplicación de ley, respuesta a incidentes y otros tipos de investigaciones. La guía se centra en las características de los teléfonos móviles, incluyendo teléfonos inteligentes con capacidades avanzadas. También cubre las disposiciones que deben tenerse en cuenta durante el curso de una investigación del incidente.

La guía está dirigida a hacer frente a circunstancias comunes que se pueden encontrar por el personal de seguridad de la organización y los investigadores policiales, relativa a los datos electrónicos digitales que

residen en los teléfonos celulares y los medios electrónicos asociados. También tiene por objeto complementar las directrices existentes y profundizar en temas relacionados con los teléfonos celulares y su examen y análisis.

5.8.3. Metodología de análisis forense de la Red Europea de Institutos de Ciencias Forenses (ENFSI)

Guidelines for best practice in the Forensic Examination of Digital Technology. Esta guía de mejores prácticas en un examen forense digital se centra en los requisitos para la recuperación de los datos de los siguientes dispositivos digitales:

- Medios de comunicación relacionados con la informática: discos duros, unidades USB, medios de comunicación inteligentes, memoria flash, disquetes y otros medios de almacenamiento como discos ópticos, cintas.
- Teléfonos móviles.
- Los datos de telecomunicaciones (por ejemplo, análisis de célula de la Web).
- Los dispositivos digitales asociados a los coches (por ejemplo, dispositivos GPS y electrónica de vehículos).

5.9. Herramientas para análisis forense

Existen una variedad de herramientas para recuperar evidencia y recopilar información de una manera exacta. Clasificándolas en herramientas comerciales y herramientas gratuitas y/o de código abierto.

Lo invito a revisar algunas de estas herramientas. Es importante que usted trate de conseguir estas herramientas para su mejor comprensión pues algunas de ellas están disponibles en la Web. Póngase en contacto con el tutor para que le ayude con los sitios donde se puede conseguir estas herramientas. A continuación, se detallan algunas de ellas.

5.9.1. Herramientas comerciales

En (Jaramillo & Guamán, 2017) se hace un estudio de estas herramientas, entre las herramientas comerciales tenemos:

- a. **Oxygen forensic Suite.** Oxygen Forensics es un producto líder en el análisis forense de dispositivos móviles, utilizado por auditores y equipos de TI que gestionan sistemas de telefonía corporativos. Es una completa aplicación forense que te ofrecerá la posibilidad de extraer y analizar información desde smartphones, teléfonos celulares, PDAs y otros dispositivos móviles. Utilizando protocolos propietarios de bajo nivel, Oxygen Forensic Suite puede extraer muchos más datos que son generalmente extraídos por otras herramientas forenses, especialmente para smartphones (Oxygen Forensics, 2021), en este [video](#) usted puede ver cómo realizar la instalación de la herramienta.
- b. **MOBILedit:** MOBILedit es una plataforma que funciona con una variedad de teléfonos y smartphones, explora el contenido del teléfono a través de una estructura de carpetas de Outlook como la EM. Esto permite que la copia de seguridad de la información almacenada en el teléfono, guardarla en un PC o copiar los datos a otro teléfono mediante la función de copiadra teléfono. Es una herramienta confiable de análisis forense en celulares utilizada en más de 70 países y reconocida por el Instituto Nacional de Estándares y Tecnología. Permite extraer todo el contenido del teléfono y genera un reporte en cualquier idioma, listo para su presentación en una audiencia (MOBILedit, 2020). En el siguiente [video](#) puede ver el trabajo de esta herramienta.
- c. **EnCase Forensic;** EnCase es una *suite* de informática forense. El software viene en varias formas diseñadas para forense, seguridad cibernética y e-discovery uso. La empresa ofrece capacitación EnCase y certificación. Los datos recuperados por EnCase ha sido utilizado con éxito en los diferentes sistemas judiciales de todo el mundo, como en los casos del asesino BTK y David Westerfield (Encase, 2018). Revise el [video](#) sobre su funcionamiento.

5.9.2. Herramientas no comerciales, open source

Entre las herramientas no comerciales y *open source* (código abierto) se ha examinado las siguientes:

- a. **The Sleuth Kit open source – Autopsy**, es una aplicación de análisis forense digital y de interfaz gráfica para el Sleuth Kit y otras herramientas de análisis forense digital. Ha sido utilizado por algunas instituciones públicas en casos oficiales, así como examinadores corporativos para investigar lo ocurrido en un computador. Se puede utilizar para recuperar fotos desde componentes como memoria de la cámara digital. Es una colección de herramientas forenses para entornos UNIX/Linux/windows. Puede analizar archivos de datos de evidencias generadas con utilidades del disco. Puede revisar el [video](#) sobre el uso de la herramienta.

- b. **Android SDK**: el SDK (Software Development Kit) de Android, incluye un conjunto de herramientas de desarrollo. Comprende un depurador de código, biblioteca, un simulador de teléfono basado en QEMU (emular de un sistema informático completo), documentación, ejemplos de código y tutoriales. Las plataformas de desarrollo soportadas incluyen Linux, Mac OS o posterior y Windows. La plataforma integral de desarrollo soportado es Eclipse junto con el complemento ADT (Android Development Tools plugin), aunque también puede utilizarse un editor de texto para escribir ficheros Java y Xml y utilizar comandos en un terminal (se necesitan los paquetes JDK, Java Development Kit y Apache Ant) para crear y depurar aplicaciones. La manera natural de interactuar con el teléfono para hacer análisis forense a los dispositivos móviles con sistema operativo Android, a nivel consola es lanzar comandos mediante Android Debug Bridge (ADB) como usuario root (SDK, 2019). Lo invito a revisar este [webbinar](#) sobre el análisis de dispositivos móviles.

5.10. Plan de respuesta a incidentes informáticos

En este apartado hacemos llegar algunas recomendaciones al momento de presentarse un incidente informático de la empresa, pues muchas veces se piensa que quienes pertenecen al departamento de TI de una empresa lo debe conocer todo o asumimos que es una obligación por parte nuestra:

- Actuar de forma metódica es decir primeramente determinar cuál es el problema y si este puede pasar a un litigio civil, pues entonces considerar que si se altera la evidencia esta dejará de ser útil.

- Si no se tiene pleno conocimiento del trabajo de las herramientas buscar a empresas externas que puedan prestarnos la ayuda necesaria.
- No altere la escena, es importante recordar la utilización de una metodología para seguir un camino lógico de actividades. Es importante.

De la misma manera se puede trabajar con un plan de respuesta a incidentes informáticos. En (ECALDIMA, n.d.), nos listan 6 pasos para la elaboración de un Plan de incidentes informáticos, que los vamos a mencionar a continuación:

1. *Involucrar al equipo informático de respuesta a incidentes*: con las personas y la experiencia adecuada. frente al incidente el primer paso es crear un equipo multidisciplinario contando con un líder responsable.
2. *Identificar el incidente y establecer el tipo y la fuente del ataque*: Ante cualquier signo de amenaza, el equipo de TI debe actuar rápidamente
3. *Evaluuar y analizar el impacto del ataque*: el análisis debe descubrir el tipo de ataque, su impacto y los servicios que podría haber afectado.
4. *Contención, eliminación de amenazas y recuperación*: en esta fase incluye bloquear la propagación del ataque, así como restaurar los sistemas al estado de operación inicial
5. *Notificación e informes*: se debe documentar los hallazgos, el impacto, la resolución del problema y la estrategia de recuperación presentando un informe pormenorizado.
6. *Realizar una revisión posterior al incidente*: en este punto se deben poner práctica las lecciones aprendidas documentando las mismas, esto debe ser un paso obligado en el plan de respuesta de incidentes, además, el de ejecutar las herramientas de seguridad actualizadas y efectivas, corregir problemas en los servidores, actualizar aplicaciones, etc.

Le invito a revisar las siguientes páginas para reforzar este tema pues se presentan algunas alternativas que pueden ser consideradas, [GoAnywhere](#) donde también encontrara plantillas que le pueden ser de utilidad al momento de elaborar el plan. Otra alternativa lo puede encontrar en

[securitymetrics](#) donde también nos presentan algunas recomendaciones para la elaboración del plan. Finalmente el [CSO](#) también nos presentan pasos para la elaboración del plan, reviselos le será de mucha utilidad.



Hemos terminado esta semana de trabajo, estos temas son muy interesantes ¿Cómo le fue con su comprensión? Existió algunos temas que le resultaron familiares, es importante profundizar en aquellos temas que no han quedado claro. No dude en escribir a su profesor tutor por los diferentes medios de comunicación. Ayúdese de las tutorías para despejar sus dudas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

Lecturas recomendadas:

- Métodos y herramientas para el análisis forense de dispositivos móviles, Susana Herrera, Liliana Figueroa, Daniel Ghunter, Cecilia Lara, Graciela Víaña, Analía Méndez, Norma Lesca.
- Elaboración de un marco de trabajo estandarizado para el análisis forense de la evidencia digital en procesos civiles y penales en el Ecuador para ser utilizado por los Peritos acreditados en Informática por el Consejo de la Judicatura del Ecuador. Loarte Cajamarca, Byron Gustavo; Grijalva Lima, Juan Sebastián.

Videos recomendados:

- Un video explicativo de como buscar [archivos digitales mediante OSINT](#)

▪ Actividad 1

Busque dos herramientas open source y encuentre una lista de las actividades que usted podría realizar con las mismas busque información de informes en la Web. Si desea puede instalarlas. ¿Estas

herramientas pueden encontrar un archivo que ha sido eliminado?
¿Las dos herramientas permiten encontrar las aplicaciones que han sido eliminadas, se puede determinar la fecha?

- **Actividad 2**

Usted podrá encontrar en el entorno virtual de aprendizaje un video explicativo de cómo usar la herramienta *mobil-edit*, el mismo que le servirá como base para la elaboración de la actividad calificada. Familiarice con la herramienta, descargue la misma desde el sitio oficial y replique lo que se muestra en el video.

Una vez que ha estudiado los conceptos relacionados con la Unidad 3, le invito a desarrollar la Autoevaluación con el fin de evaluar los conocimientos adquiridos hasta el momento. Posterior a eso usted podrá encontrar al final de este Texto Guía la solución a cada una de las preguntas.

¡Éxitos en la autoevaluación!



Autoevaluación 5



Una vez que ha estudiado los conceptos relacionados a la unidad 3, le invito a desarrollar la autoevaluación con el fin de evaluar los conocimientos adquiridos hasta el momento. Posterior a eso, usted podrá encontrar al final de este texto-guía la solución a cada una de las preguntas.

¡Éxitos en la autoevaluación!

- 1. Se ha detectado que se envió un correo ofensivo y luego de eso fue borrado, ¿este es un tipo de análisis forense de?**
 - a. Sistemas.
 - b. Redes de ordenadores.
 - c. Sistemas embebidos.
- 2. Las herramientas utilizadas y los resultados obtenidos deben estar bien documentados. Se basa en el principio de:**
 - a. Controlar la cadena de custodia.
 - b. Evitar la contaminación.
 - c. Actuar metódicamente.
- 3. Dentro de los usos de la informática forense está el de detectar el acoso, estamos hablando de:**
 - a. Temas corporativos.
 - b. Persecución criminal.
 - c. Litigación civil.
- 4. Uno de los incidentes informáticos donde se obstaculiza las aplicaciones mediante el agotamiento de recursos se relaciona con:**
 - a. Acceso no autorizado.
 - b. Código malicioso.
 - c. Denegación de servicio.

- 5. ¿Cuál de las siguientes herramientas es de código libre?**
 - a. Autopsy.
 - b. Oxigen.
 - c. EnCase Forensic.
- 6. Dentro de los usos de la informática forense está el fraude que se realizó a un cliente de una institución bancaria, esto hace referencia a:**
 - a. Temas corporativos.
 - b. Litigación civil.
 - c. Persecución criminal.
- 7. En una de las fases para el manejo de incidentes informáticos hablamos de averiguar y evaluar las condiciones de un posible incidente, hace referencia a la fase de:**
 - a. Contención.
 - b. Detección.
 - c. Preparación.
- 8. Dentro de las fases del manejo de incidentes informáticos, encontramos varias fases. En qué fase se debe realizar la formación del equipo de manejo de respuesta a incidentes.**
 - a. Preparación.
 - b. Detección
 - c. Análisis.
- 9. ¿En cuál de las metodologías de análisis forense se expresa: "Las personas que realicen un examen de la evidencia digital debe ser entrenado para ese propósito".**
 - a. OASAM.
 - b. NIJ.
 - c. NIST.

10. ¿En cuál de las metodologías de análisis forense se expresa:

“En esta categoría se incluirán vulnerabilidades que tienen un componente más centrado en el propio diseño que la codificación”.

- a. OASAM.
- b. NIJ.
- c. NIST.

Puede verificar las respuestas de esta autoevaluación al final del Texto Guía.

[Ir al solucionario](#)

Si su puntaje no es bueno, es importante que vuelva a revisar los contenidos de la unidad y los recursos de aprendizaje, no olvide que puede interactuar con su tutor por cualquier medio de comunicación que brinda la UTPL para que aclare sus inquietudes.

Se ha preguntado alguna vez ¿Cómo las empresas vuelven a la normalidad si un hacker saca de línea su principal sistema informático? Podemos tomar como ejemplo que en un banco dejan de funcionar por 4 horas los servicios en línea que presta, debido a que un atacante, pudo de alguna manera ingresar al sistema, no solo robar información quizá de clientes, sino que también provocó un daño (más adelante lo llamaremos incidente de seguridad). ¿Cómo procede el banco para volver a la normalidad? ¿Qué hace al respecto? ¿Hay un equipo especializado para eso? Al finalizar el estudio de esta unidad usted podrá dar respuesta a estas preguntas. Le invito a leer comprensivamente esta unidad y a utilizar los recursos como lecturas complementarias y desarrollar actividades de aprendizaje propuestas para que pueda afianzar sus conocimientos.

¡Éxitos en el estudio de esta unidad!



Semana 13 y 14

Unidad 6. Gestión de la continuidad de negocio

Existen interrupciones o incidentes derivados por algunos factores que afectan el desarrollo normal de los procesos principales de una organización o de sus sistemas críticos, de aquí la importancia de tener implementado un proceso de gestión de continuidad de negocio y sobre todo de identificar las actividades principales para volver a la normalidad, procesos o sistemas que fueron interrumpidos. Algunas organizaciones junto con un sistema de gestión de continuidad de negocio consideran crear un equipo a cargo de ayudar contra estos incidentes, sobre todo incidentes de seguridad, como la creación de un CSIRT.

6.1. ¿Qué es la gestión de continuidad de negocio?

En las primeras unidades del texto guía se ha revisado temas respecto a seguridad de la información y a la gestión de riesgos, tomando en cuenta siempre en que la organización busca cuidar sus principales y más valiosos activos.

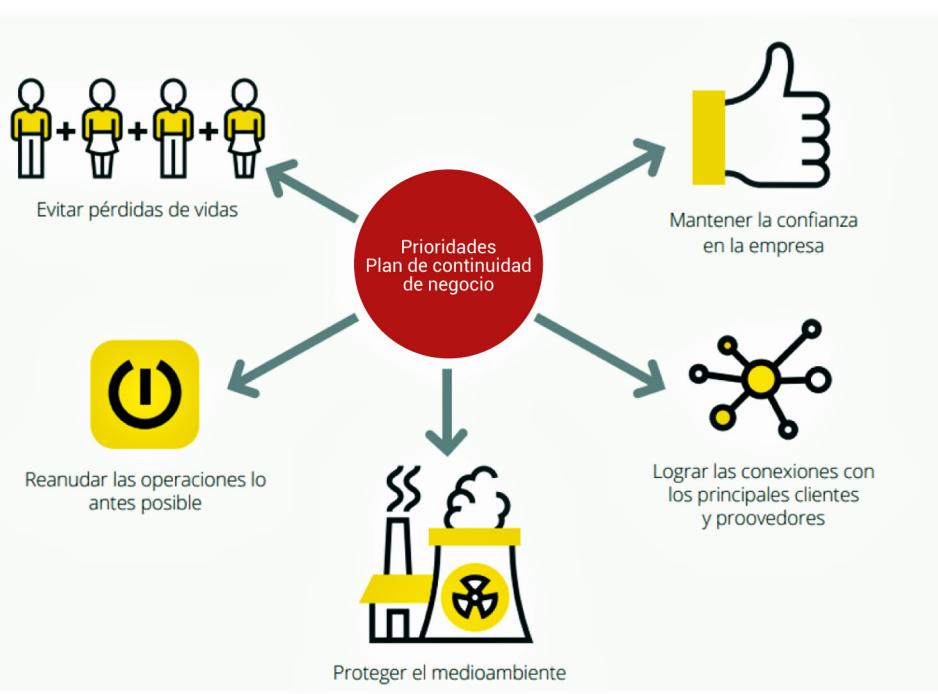
Se ha preguntado quizá para qué más sirve el proceso de asegurar la información y el proceso de gestión de riesgos, estos dos importantes

procesos tendrán resultados, los mismos que se pueden utilizar para empezar actividades que nos orienten a crear otro proceso igual de importante, como es el proceso de gestión de continuidad de negocio. ¿Qué sucede si por una vulnerabilidad una amenaza se materializa y afecta principalmente a los sistemas críticos de la organización? Y si sucediera, ¿Cómo volvemos los procesos o el sistema a la normalidad? ¿Qué tiempo se debe esperar? ¿Qué recursos se deben utilizar?

Para entender el proceso de gestión de continuidad de negocio partamos desde lo que menciona (Johanna Cárdenas Solano et al., 2014) que es la combinación entre actividades de prevención de riesgos y de recuperación de desastres que ayuden a evitar la indisponibilidad de los servicios y actividades del negocio. Hay dos enfoques en este proceso el uno es buscar proteger lo máximo posible los procesos o activos críticos de la organización del impacto al afectarse principalmente por fallas, amenazas o desastres y el otro enfoque es que se hace es si en caso ya han suscitado pérdidas, entonces ayudar a recuperar estos activos afectados y ayudar a restablecer el funcionamiento normal. En la figura 50 podemos ver las prioridades del plan de continuidad de negocio o el proceso gestión de continuidad de negocio.

Figura 50.

Prioridades del plan de continuidad de negocio



Nota. Tomado de INCIBE, 2017.

Le invito a profundizar sus conocimientos acerca de los tipos de Plan de continuidad:

6.1.1. Tipos de plan de continuidad

Existen tres tipos de plan de continuidad de negocio, según (Instituto Nacional de Ciberseguridad INCIBE, 2017) estos son:

- **Plan de Continuidad de Negocio (PCN)** se enfoca en la continuidad de negocio desde algunos ámbitos por ejemplo infraestructura de TI, infraestructura física, recursos tecnológicos, recursos humanos, etc. Cada uno de estos ámbitos requerirá de su propio plan, ya que no es lo mismo que se afecte un recurso humano de un recurso tecnológico.
- **Plan de Continuidad TIC** se enfoca solamente en el ámbito de las TIC de una organización y su recuperación si existe una falla o desastre, dentro de este plan puede estar la recuperación de infraestructura de TIC y de procesos de TIC.

- **Plan de Recuperación ante Desastres (PRD)** Se enfoca en la recuperación en un ámbito más técnico, tomando en cuenta los datos, incluyendo software y hardware críticos para que la organización pueda continuar con sus operaciones, sea que hayan sido detenidas por un fallo humano o natural.

Dentro del plan de continuidad de negocio se encuentran incluidos el plan de continuidad de TIC y el de recuperación ante desastres, ya que la estructura organizacional está compuesta de algunos elementos.

En cualquier de los casos saber establecer un buen plan de continuidad de negocio tiene que ver también con dos procesos que ya han sido en algunos casos desarrollados en la empresa y estos son el proceso de seguridad de información y gestión de riesgos.

El proceso de seguridad de la información debe ser considerado para establecer la continuidad de negocio y con ello según explica (Johanna Cárdenas Solano et al., 2014) se toman encuentra algunas consideraciones como las siguientes:

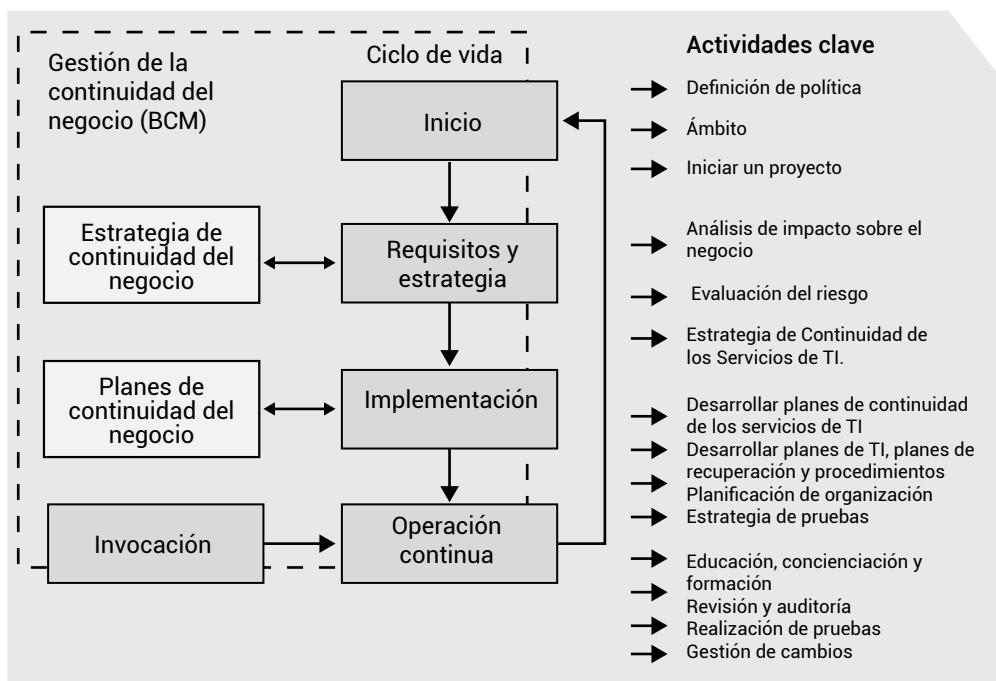
- Identificación de riesgos en la organización.
- Identificación de procesos y activos críticos.
- Comprensión del costo del impacto si se produce un incidente de seguridad
- Medidas preventivas, correctivas y detectivos implementadas
- Recursos implicados para las medidas.
- Requisitos de seguridad considerados e incluidos.
- Identificación de pruebas de los controles y su mantenimiento.

El análisis de riesgos ayudará a establecer un plan basado en posibles escenarios para saber las estrategias y rutas a seguir para seguir con la continuidad de negocio.

Para una mayor comprensión de lo que es la gestión de continuidad de negocio nos vamos a referir a ITIL v3 que propone un proceso de gestión de continuidad del servicio de TI conocido por sus siglas (ITSCM) y según (Van Bon et al., 2017) su objetivo es dar soporte al proceso de continuidad de negocio, dando garantía que toda la infraestructura de TI y de servicios de TI funcionen en ciertos plazos de tiempo que se hayan acordado en la organización. En la figura 51 pueden las etapas y actividades de la ITSCM.

Figura 51.

Ciclo de vida de la continuidad de negocio



Nota. Tomado de Van Bon et al., 2017.

6.2. Plan de continuidad del negocio

Existen algunos criterios y factores que se deben tomar en cuenta para garantizar la continuidad de una organización, estos criterios están dentro de un proceso de varias fases, conocido como Fases del Plan de Continuidad de Negocio ver figura 51.

Aunque la planificación de continuidad de negocio debe ser un plan integral que cubre todos los aspectos críticos de la organización, es preferible siempre para que se tenga éxito, que se identifique todas las personas involucradas y los recursos. También es importante tener claro que el apoyo debe ser desde el Gobierno de la Organización, es decir el plan o desarrollo del plan debe ser apoyado al 100% desde la Gerencia o cabeza principal de la organización.

Tabla 26.

Fases del plan de continuidad de negocio

Determinación del alcance	Identificar las áreas más importantes en donde se empezará la continuidad.
Análisis de la organización	Identificar los procesos de negocio críticos y los recursos que lo soportan.
Determinar la estrategia de continuidad	Identificar la capacidad de dar respuesta a un incidente o de recuperar los activos involucrados.
Respuesta de contingencia	Implantación de iniciativas para la recuperación de los entornos y se documenta.
Prueba, mantenimiento y revisión	Desarrollo de planes de mantenimiento y pruebas.
Concienciación	Comunicar el plan de continuidad de negocio a todo el personal de la organización.

Otro de los puntos a considerar cuando se planifica el proceso de gestión de continuidad de negocio es que permite que se involucre tanto a personal que realice este plan como proyecto, como a quienes en su momento lo ejecutarán. Enseguida se puede detallar que va en cada parte de este plan del proceso de gestión de continuidad de negocio.

6.2.1. Determinación del alcance y análisis de la empresa

Esta fase muy parecida a las fases de determinación del alcance tanto del proceso de seguridad de la información como del de gestión de riesgos donde se determina el área donde iniciará o se basará el plan de continuidad, sobre todo con la intención de establecer costos, ya que al igual que otros procesos de gestión, establecer la continuidad de negocio es un proyecto que demanda costos y recursos.

Para empezar a desarrollar este plan, se debe tener sus objetivos claramente definidos y que se deben considerar en este alcance, una de las preguntas que puede ayudar a identificar a estos objetivos es ¿Qué estamos tratando de resolver?, pero la respuesta debe ser muy específica y detallada, tomando en cuenta desde la perspectiva de incluso que recursos están involucrados desde ese proceso, activo o área que queremos hacer la continuidad.

Es importante que junto con tener claros los objetivos de este plan que se lo propone al inicio como proyecto y que empieza por estimar su alcance, es tener claro los requisitos de estos, es decir lo que se necesitará tener disponible en la organización para que estos objetivos se cumplan. Por

ejemplo, si una de las prioridades de la organización es la de tener 100% disponible su aplicación web de ventas, pues tendrá que ver qué datos maneja y debe cuidar, qué recursos de TI necesita para que esté operativa y funcional, qué personas están involucradas y a quiénes afecta incluyendo clientes de la organización. Estos requisitos se dividen en tres categorías como se muestra en la tabla.

Tabla 27.

Requisitos de la continuidad de negocio

Requisitos comerciales	Ayuda a determinar qué necesita la organización para sobrevivir a una interrupción, se enfocarán a entender los componentes básicos de la organización y como se interrelacionan para saber las áreas claves a priorizarse, están relacionados con: tiempos de respuesta, disponibilidad de datos y la tolerancia al tiempo de inactividad.
Requisitos funcionales	Detallan cosas como qué procesos, métodos y los recursos deben estar disponibles durante y después de una interrupción del negocio.
Requisitos técnicos	Se refiere a aplicaciones, infraestructura de TI, de red, hardware, software, etc. que se necesita durante y después de la interrupción de un proceso o activo.

Para saber cómo manejar la gestión de continuidad como un proyecto es importante conocer cómo se lleva a cabo la gestión de proyectos básica.

En cuanto a determinar el alcance de la continuidad a los sistemas de información o procesos críticos, es decir, los que en caso haya un fallo o un desastre el impacto sea demasiado dañino para la organización. El enfoque del alcance se lo puede enfocar desde algunas perspectivas, como indica (Instituto Nacional de Ciberseguridad INCIBE, 2017):

- Perspectiva por activo: la continuidad está basada en un grupo de activos y de ellos se levanta los procesos que a los que estos activos apoyan.
- Perspectiva por proceso: la continuidad está basada en un proceso.

En la tabla se puede explicar la diferencia del alcance en cualquiera de estas dos perspectivas.

Tabla 28.

Ejemplos de perspectivas para definir la continuidad de negocio

EJEMPLO

El entorno virtual de aprendizaje, que es crítica como herramienta de apoyo para el proceso de enseñanza aprendizaje de la modalidad abierta y distancia de la UTPL.

Perspectiva por activo

El análisis para la continuidad se centrará en el activo, es decir en sistema o aplicación Web que es el Entorno Virtual de Aprendizaje, a partir de aquí se determinan las dependencias de la organización que dependen de este activo o utilizan este activo.

Perspectiva por proceso

El análisis para la continuidad se centrará en la mejora del proceso de enseñanza aprendizaje de la MAD UTPL y en el que una parte de este proceso es el apoyo de una herramienta como el EVA y otros activos.

Es recomendable por varios expertos en temas de gestión de continuidad de negocio que se empiece la continuidad siempre con un enfoque o perspectiva por proceso y que los ámbitos a cubrir sean las TI o TIC utilizadas como apoyo para la operatividad de este proceso.

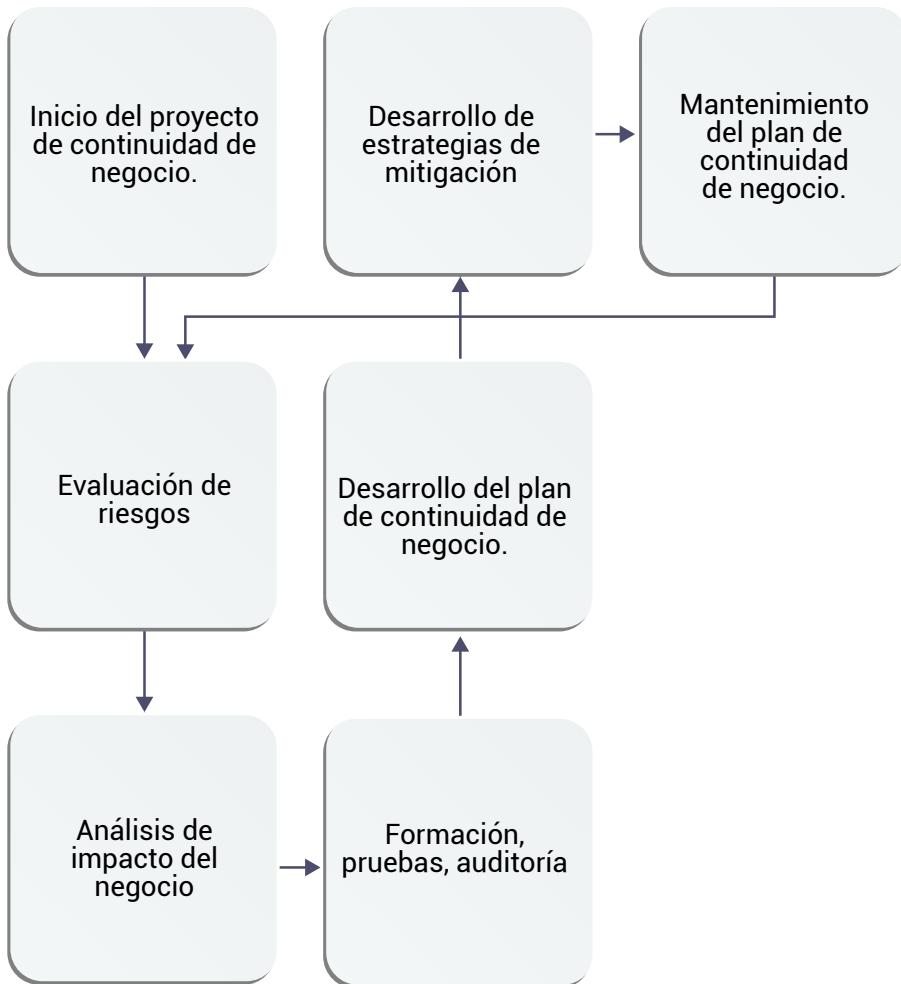
Una vez determinado el proceso se debe analizar todos los elementos que forman parte de este proceso, es decir, determinar los recursos que necesita, tanto de TI como humanos, la infraestructura, todo lo que apoya para que este proceso funcione, qué información es procesada y cuáles son los resultados de estos. También es importante entender el objetivo de este proceso.

Empiezan las entrevistas como para entender este proceso de estas reuniones según (Instituto Nacional de Ciberseguridad INCIBE, 2017), se determina si este proceso depende de proveedores, el personal implicado, las aplicaciones que se utilicen en el proceso, qué información manipula, qué tecnologías utiliza. También se evalúa qué controles sean preventivos, defectivos o correctivos están en este proceso o en las aplicaciones o TI que utilice. Por ejemplo, un tipo de control que puede estar establecido es que se saquen respaldos de la información que se manejen en los sistemas que apoyan a los procesos críticos.

6.2.2. La evaluación de riesgos como base para establecer el plan de continuidad de negocio

Luego de establecer el alcance y de identificar desde donde se empezará el proyecto de continuidad de negocio, se debe hacer el análisis de riesgo, como se puede ver en la figura 52.

Figura 52.
Fases de proyecto de continuidad de negocio



Nota. Adaptado de Snedaker & Rima, 2014.

En la Unidad 2 del texto guía se estudió el proceso de la gestión de riesgos, ahora en este punto lo que queda decidir es si se utilizará un método cuantitativo o cualitativo para valorar el riesgo o los riesgos identificados del proceso crítico que se identificó y en el que se basará el plan o proyecto

de continuidad y si el valor del riesgo estará basado en el análisis de vulnerabilidades, en el impacto que repercuten en algún activo u orientado a amenazas. El proceso de gestión de riesgos enfocado en un plan de continuidad evalúa en qué probabilidades o circunstancias los sistemas o procesos críticos pueden paralizarse y se debe considerar que siempre por alguna u otra razón estos procesos se pueden paralizar.

El costo de las interrupciones varía, generalmente en correlación directa con el tiempo que el sistema o proceso está inactivo y si el tiempo de inactividad es planificado o no. Considere el siguiente ejemplo:

Si una aplicación Web está inactiva durante 5 minutos mientras se reinicia debido a una actualización de este, el costo es insignificante.

Si la aplicación Web deja de funcionar por varios días por el ataque de un *hacker* quien afectó a la base de datos, el costo es elevado totalmente.

El análisis del costo debe ser un punto primordial para estudiar la comparación debe ser entre el costo del tratamiento de riesgo con el costo de la pérdida de los activos o del activo que se ve afectado. Por ejemplo:

Se debe comparar o analizar cuánto cuesta instalar un sistema de extinción de incendios en la organización, contra el costo de si al suceder un incendio dañe la infraestructura de TI, haya pérdidas incluso de vidas humanas.

En la unidad 1 y 2 del texto base se conocieron conceptos y el contexto de utilizar las definiciones de riesgo y amenaza. Pero cuando estamos en definiendo el plan de continuidad de negocio, se debe tomar en cuenta el *riesgo comercial*, (Snedaker & Rima, 2014) se refieren a este riesgo como el proceso de identificar, controlar y eliminar o minimizar eventos inciertos que pueden afectar a las organizaciones. Incluye análisis de riesgo, análisis de costo-beneficio, selección, implementación y prueba de estrategias seleccionadas y mantenimiento de esas estrategias a lo largo del tiempo. Así mismo es esta etapa/fase/paso se debe hacer un adecuado tratamiento de los riesgos, algo que se estudió previamente en la unidad 2.

Otra parte sumamente importante para considerar es que, aunque hay riesgos generales a tomar en cuenta en un plan de continuidad, con enfoque a sistemas de información, se debe considerar como prioridad el tratar a los riesgos de TI y uno de los mayores riesgos de TI de una organización son los datos o la información que es obtenida, procesada y almacenada utilizando infraestructura de TI. Al tratar los riesgos de TI organizacionales lo que se está logrando o consiguiendo es que los Sistemas de información tengan un nivel de seguridad más alto.

Sea cualquier tipo de riesgo no podemos dejar pasar por alto dentro de un plan de continuidad de negocio, aquellos riesgos en los que la mano del hombre no está inmiscuida, es decir los riesgos o *amenazas naturales* a los que toda organización, quiera o no está expuesta y que en caso de materializarse afectan, a veces, de una manera implacable a los activos de la empresa, sean personas, procesos, tecnologías e infraestructura. Como puede ser el fuego, las inundaciones, terremotos e incluso pandemias.

De esta fase lo que se obtiene como resultado final es una lista de riesgos identificados, junto con la evaluación de amenazas y vulnerabilidades y el enfoque de desarrollo de una estrategia de tratamiento de riesgo.

6.2.3. Análisis de impacto de negocio

Es el proceso de comprender el impacto de una interrupción en los procesos críticos de la organización, para ello se toman en cuenta algunos criterios: servicio al cliente, operaciones internas, legales y financieras, así como funciones comerciales y críticas vinculadas con sistemas de TI específicos. Para ello se requiere desarrollar algunas actividades como son:

- Identificar las funciones y los procesos críticos.
- Establecer requisitos para la recuperación de negocio.
- Determinar las interdependencias de los recursos o activos.
- Determinar el impacto en las operaciones.
- Desarrollar prioridades y clasificación de procesos y funciones de negocio.
- Desarrollar requisitos de tiempo de recuperación de los procesos.
- Determinar el impacto financiero, operativo y legal de la interrupción en el negocio.

El resultado de estas actividades junto con la evaluación de riesgos nos ayuda a determinar las mejores estrategias de mitigación. Es importante

en todo caso cuando se hace el estudio de los procesos críticos, antes que evaluar su impacto y categorizarlos de tal manera que tengamos una idea de que procesos críticos evaluar primero.

Le invito a profundizar sus conocimientos acerca de este importante tema:

Al igual que valorar los riesgos con la estimación de probabilidad e impacto, se puede tener una categoría para los procesos a tratar y poder tener un orden de prioridad. En la tabla 29 se puede especificar cuatro categorías.

Tabla 29.

Categoría de procesos para la continuidad

Misión crítica

- Procesos críticos que tienen el mayor impacto de las operaciones de la organización y la necesidad de recuperación.
- Este tipo de interrupción puede poner en peligro la existencia de la organización. Esta interrupción tiene serias ramificaciones de seguridad, legales, operativas y financieras.
- La tolerancia para tal interrupción es muy baja y el tiempo de recuperación requerido a menudo se describe en términos de horas.

Importantes

- Procesos importantes que si son interrumpidos su impacto es a largo plazo. Por ejemplo, el acceso a Internet, bases de datos, sistemas de soporte que ayudan con reportes.
- El tiempo de recuperación requerido se mide en días o semanas.

Menores

- Procesos creados para tratar problemas menores y recurrentes.
- Se pueden recuperar a largo plazo.
- El identificarlos nos pueden ayudar a terminar con procesos obsoletos.
- El tiempo de recuperación requerida se mide en semanas o meses.

Una vez categorizados los procesos entonces tenemos que relacionarlos con los requisitos de tiempo de recuperación, detallados en la figura 52.

Tabla 30.

Requisitos del tiempo de recuperación

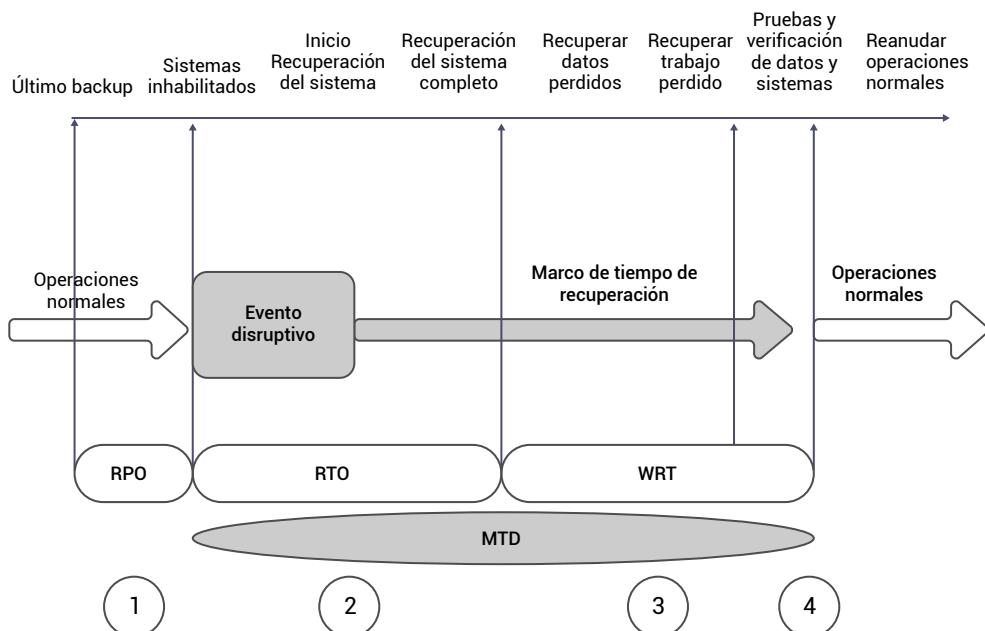
Tiempo de recuperación RTO	Es el tiempo en que un proceso se paraliza (puede ser por consecuencia de un ataque, fallo o desastre) antes de que sea puesto en funcionamiento nuevamente. Lo determina el personal técnico
Recursos implicados en el proceso	Se refiere a todos los recursos tecnológicos implicados en el proceso, software, hardware, información, recursos humanos, infraestructura, etc. que sirven de apoyo para el proceso.
Tiempo Máximo Tolerable de Caída MTD	Es el tiempo en que el proceso puede permanecer paralizado antes de que haya consecuencias en la organización.
Tiempo de recuperación del trabajo WRT	SE necesita tiempo para que los procesos críticos vuelvan a funcionar una vez que los sistemas o IaTI es restaurada, por ejemplo, los datos deben probarse para que los backups sean correctos.
Determinar dependencias de otros procesos o proveedores	Existen procesos con dependencias en otros proveedores de los que deben tener un plan de recuperación, esto con el propósito de verificar que los proveedores pueden apoyar si el proceso se paraliza.
RPO (Recovery Point Objetive)	Que cantidad perdida de datos esta la organización dispuesta a tolerar, por ejemplo, desde que el proceso se paralizó y el último backup del mismo. ¿Cuántos datos se pierden?

Nota. Adaptado de Shedaker & Rima, 2014.

En la figura 53 se puede observar la línea de tiempo de recuperación del negocio:

Figura 53.

Línea de tiempo de recuperación de negocio



Nota. Tomado de Snedaker & Rima, 2014.

Para pasar a la etapa de desarrollo de estrategias de mitigación que es cuando ya evaluamos el impacto, necesitamos tener algunos datos, estos datos se los puede obtener identificándolos a partir de los elementos de que conforman un sistema de información, es decir, analizando la información que procesa el *software*, el *hardware* que apoya al funcionamiento, la infraestructura física y de TI necesaria y las personas.

De todo este proceso de análisis de impacto como resultado tenemos el Reporte de análisis de impacto donde se deben incluir los siguientes puntos:

- Procesos y funciones clave
- Interdependencia de procesos y recursos
- Dependencias de TI
- Criticidad e impacto en las operaciones
- Funciones, puestos, habilidades, conocimientos y experiencia clave necesarios del personal
- Requisitos de tiempo de recuperación
- Recursos de recuperación
- Acuerdos de nivel de servicio

- Tecnología (tecnología de TI y no TI)
- Impactos financieros, legales, operativos, de mercado y de personal
- Procedimientos alternativos
- Datos comerciales y registros de claves
- Informes (auditorias anteriores)
- Impacto competitivo
- Impacto inversor/mercado
- Impacto en la percepción del cliente

6.2.4. Determinación e implementación de la estrategia de continuidad

Es la fase más importante de proceso de continuidad de negocio, donde se determinan las soluciones alternas para poder continuar o recuperar los procesos de la organización y está basada en desarrollar estrategias para aceptar, evitar, reducir o transferir los riesgos relacionados con posibles interrupciones del negocio.

La evaluación de riesgos y los datos del análisis de impacto empresarial más los datos de mitigación de riesgos, se desarrollan las estrategias para gestionar los riesgos de forma adecuada para su empresa, esta estrategia creada debe cumplir con los objetivos financieros, operativos y de gestión de riesgos de la organización.

En la tabla 31 (Instituto Nacional de Ciberseguridad INCIBE, 2017) menciona la información necesaria para establecer la Estrategia de continuidad, esta información que hasta el momento ya debió ser identificada.

Tabla 31.

Elementos para definir la estrategia de continuidad



Los procesos críticos del negocio, sus tiempos necesarios de recuperación y sus requisitos de pérdida de datos.



Los recursos implicados en cada uno de los procesos: aplicaciones, etc...



Los tiempos de recuperación de cada uno de los recursos que puede garantizar nuestro personal técnico.



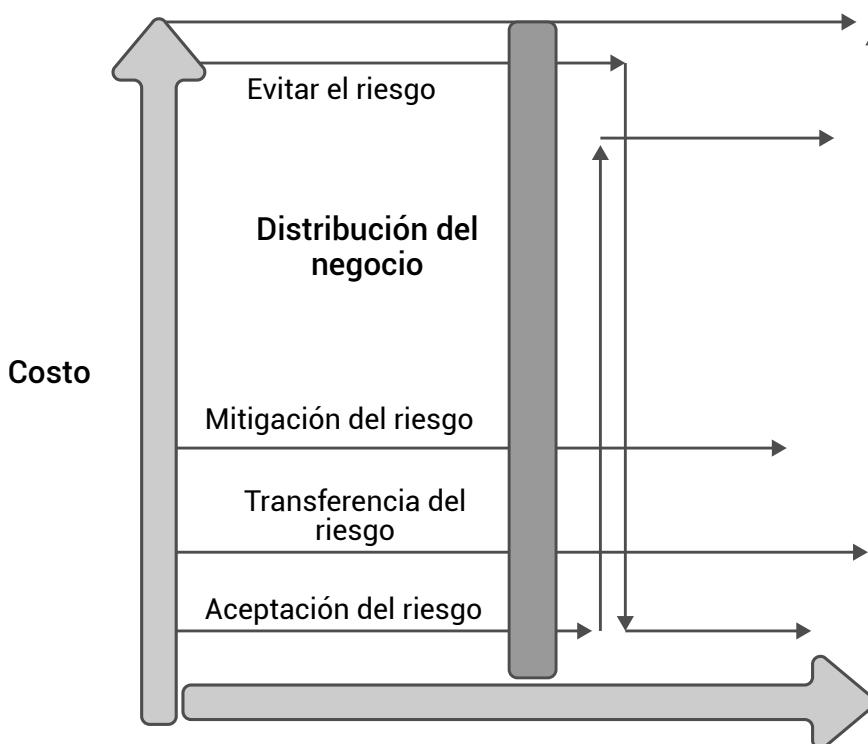
Los riesgos a los que se encuentra sometida la infraestructura TI.

Nota. Tomado de INCIBE, 2017.

Con esta información recopilada se podrá establecer cómo recuperar un sistema o el proceso como tal. Pero antes de ello es necesario recordar en esta parte las cuatro opciones que se tienen para el tratamiento de riesgo, aunque se las estudie en la unidad 2 del texto guía es importante que usted las recuerde. En la figura 54 puede observar la relación que existe entre el tiempo de tratamiento de riesgo y el costo que deberá cubrir la organización dependiendo de la opción de mitigación que escoja.

Figura 54.

Tiempo de tratamiento vs. costo



Nota. Adaptado de Snedaker & Rima, 2014.

Dentro del proceso de mitigación de riesgos otro factor a analizar el perfil de recuperación, incluidos los requisitos de recuperación, las opciones, el período de tiempo de las opciones (en comparación con el tiempo de inactividad máximo tolerable o MTD) y el costo frente a la capacidad de las opciones. Una vez que se conocen estos elementos, se puede diseñar una estrategia de mitigación de riesgos íntegra.

Lo siguiente es establecer los requisitos de recuperación que ayudan a identificar los recursos que deben ser el foco de la estrategia de recuperación incluyen instalaciones y áreas de trabajo, sistemas e infraestructura de TI, fabricación y producción (operaciones) y datos críticos/registros vitales. Los requisitos de recuperación se identifican para los procesos críticos identificados en el análisis de impacto comercial.

Con estos requisitos de recuperación se consideran algunas opciones de recuperación que dependen mucho de lo que ya se ha estudiado en los

puntos anteriores dentro de esta unidad. Cada opción de recuperación tendrá sus capacidades, como costos y cronogramas propios. Un ejemplo de opción de recuperación es contemplar el tener un sistema de *backup* en tiempo real de los sistemas críticos de la empresa.

Existen tres opciones básicas de recuperación que se pueden considerar, incluso como parte de la estrategia de mitigación. En la tabla 32 se describe estas opciones.

Tabla 32.

Opciones de recuperación

Según sea necesario	Adquirir los recursos en el momento de la interrupción. Es el caso por ejemplo si la interrupción se da por algún desastre natural, en ese caso podría ser aceptable por parte de la organización pagar los costos. Hay que tomar en cuenta, que no siempre habrá recursos disponibles, el costo puede ser elevado y hay un alto riesgo en la implementación. Una solución viable es tener a la mano siempre el contacto de proveedores y archivado de alguna manera las especificaciones técnicas de los activos.
Acordado de antemano	Se refiere a buscar un proveedor para que haga el suministro de sistemas, productos o servicios requeridos después de una interrupción de negocio. Lo importante aquí es tener SLA bien especificados para garantizar que las necesidades se cumplan y lo que se acepta por adelantado incluyendo el contrato.
Preestablecido	Son opciones de recuperación que se compran, configuran e implementan antes de una interrupción y se utilizan solo para recuperarse de esta interrupción. La ventaja es que cuando la organización sufre una interrupción esta puede recuperarse con algún tipo de sistema de recuperación previamente implementado, sin embargo, puede suceder que quizás no sufra una interrupción por lo que con el tiempo estos sistemas se vuelven obsoletos.

Nota. Adaptado de Snedaker & Rima, 2014.

Después de tener establecidas estas opciones de recuperación se evaluará el costo de cada una de las opciones, algunas opciones pueden tener varios niveles de costo/capacidad. En la mayoría de los casos, cuanto mayor sea la capacidad, mayor será el costo. En todo caso es importante que se considere que las estrategias de mitigación dependerán netamente de las limitaciones financieras de la empresa. Los puntos para considerar en la evaluación de costo de estas opciones para (Snedaker & Rima, 2014) son:

- Costo: el costo de la opción de mitigación o recuperación.
- Capacidad: las capacidades de la opción.

- Esfuerzo: la cantidad de esfuerzo que se necesitará para implementar y administrar la opción.
- Calidad: la calidad del producto, servicio o datos asociados con la opción.
- Control: la cantidad de control que la organización mantendrá sobre el proceso comercial crítico.
- Seguridad: en los casos en que la seguridad física es una preocupación, este atributo califica la seguridad de la solución.
- Seguridad: las estimaciones de seguridad física y virtual (información y acceso a la red) que proporciona la opción.

Con las opciones establecidas y mucho antes de tomar decisiones de adquisición, sobre todo, se debe revisar si existen algunos controles, es posible que ya se hayan establecido todos o una parte de estos, con ello también se encontraría áreas de la organización donde aún no se establecen los controles de recuperación para continuidad de negocio.

Finalmente concluimos esta fase con la documentación que detalle las estrategias que se tomarán en cuenta y se deberá presentar a los directivos de la organización de tal manera que incluso se aconseje hacer una auditoría.

6.2.5. Desarrollo del plan de continuidad de negocio

Como primer paso es implementar las estrategias de mitigación de riesgos escogidas e identificadas en el punto 6.2.3. Veamos las estrategias:

Por ejemplo, algunas estrategias de para la continuidad de negocios son:

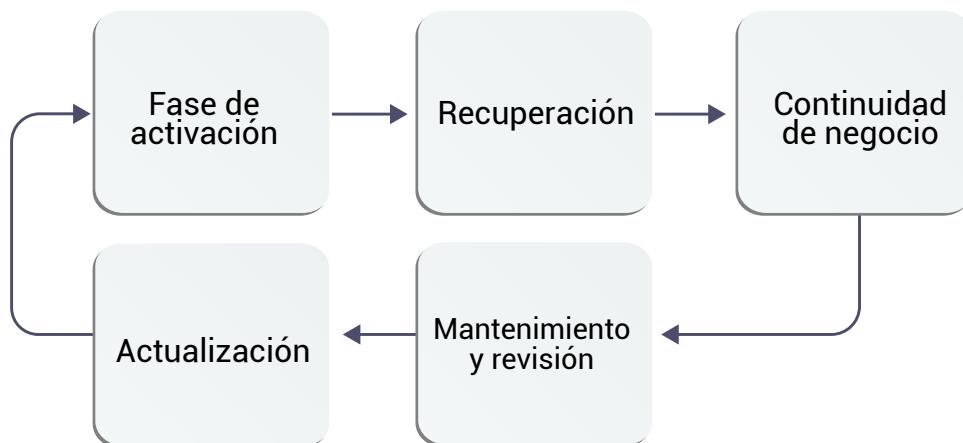
- La actualización de antivirus y de sistemas operativos.
- Revisar firewall para ver si hay puertos abiertos.
- Configurar parches de seguridad en los servidores.
- Implementar bases de datos de contraseñas encriptadas y separadas por roles.
- Implementar controles de seguridad física para todos los equipos de TI.

- Implementar políticas de caducidad de contraseñas y cambiar las contraseñas administrativas periódicamente o cuando ocurran cambios de personal.
- Implementar políticas de autenticación y contraseñas sólidas y centralizadas.
- Implementar una computadora independiente no conectada a la red para escanear todos los medios extraíbles, como unidades USB, CD-ROM o DVD, en busca de virus o malware antes de que se utilicen en la red.
- Consolidar y automatizar el análisis de registros de seguridad con un sistema o dispositivo de gestión de eventos e información de seguridad;
- Hacer copias de seguridad de sistemas y datos periódicamente en medios extraíbles y almacenar copias de seguridad fuera del sitio, o hacer copias de seguridad en una nube segura o en un proveedor de Internet.
- Mantener hardware de TI de repuesto en una ubicación externa o contratar un proveedor de nube segura de antemano para poder poner en marcha rápidamente los servidores virtuales o estaciones de trabajo necesarios para recuperar sistemas y datos alojados internamente.
- Implementar hardware de TI automatizado y monitoreo ambiental y herramientas de alerta, como monitoreo del Protocolo simple de administración de red, para eventos como discos defectuosos, mala memoria, eventos de temperatura, detección de fugas, detección de incendios, etc.
- Capacitación formal documentada para todos los empleados sobre seguridad de TI básica y procedimientos de recuperación ante desastres, generalmente como parte del proceso de incorporación de empleados o durante ejercicios de capacitación anuales.

En la siguiente figura 55 se puede observar las fases de desarrollo del plan de continuidad de negocio.

Figura 55.

Fases de desarrollo del plan de continuidad de negocio



Nota. Tomado Snedaker & Rima, 2014.

Fase de activación: Se debe definir cuándo se activará el plan y de qué manera. También se deberá desarrollar un conjunto claro de parámetros para determinar si debe activar el plan o cuándo hacerlo. Además, se debe definir cómo se activa el plan, incluido quién tiene la autoridad para activarlo y qué proceso seguirá esa persona (o personas) para iniciar las actividades. La activación incluye respuesta inicial y notificación, evaluación y escalada de problemas, declaración de desastres e implementación del plan. La fase de activación del plan debe definir varios niveles de desastre o interrupción para saber cuándo y cómo implementar el plan, estos niveles pueden ser menor, intermedia y mayor.

- **Interrupción menor:** La probabilidad de que ocurra un evento menor es alta, pero la interrupción asociada es relativamente baja. Cuando ocurre afecta solo a un componente del proceso crítico y este puede seguir operando a pesar de ello. Si sucede el fallo de un sistema se puede solucionar durante el curso normal del negocio.
- **Interrupción intermedia:** Es probable que ocurra con más frecuencia que un desastre mayor, pero obviamente con menos frecuencia que un desastre menor. Interrumpe o impacta una o más funciones de misión crítica o unidades de negocio, pero no todas. Las operaciones experimentarán una interrupción significativa; sistemas completos o múltiples sistemas pueden fallar o no estar disponibles, pero no todos.

- **Interrupción mayor:** La posibilidad o probabilidad de que ocurra este tipo de desastre es baja, pero el impacto en el negocio es extremadamente alto. Este evento interrumpe todas o la mayoría de las operaciones comerciales normales de la empresa y todos o la mayoría de sus procesos comerciales críticos. Las interrupciones ocurren porque todos o la mayoría de los sistemas y equipos han fallado o son inaccesibles.

Fase de recuperación: Es la primera fase del trabajo inmediatamente después de la interrupción o el desastre. Esta fase generalmente asume que la causa de la interrupción ha disminuido, detenido o contenido, pero no siempre. Se puede decir que los esfuerzos de recuperación tienen que ver con recuperarse de las secuelas inmediatas del evento, ya sea que el evento continúe o no. Esta fase también puede incluir la evacuación de la instalación, la remoción de equipos que se pueden recuperar rápidamente, la evaluación de la situación o el daño y la determinación de los pasos de recuperación necesarios para que las operaciones vuelvan a funcionar.

Fase de continuidad de negocio: Esta fase comienza después de la fase de recuperación y define los pasos necesarios para volver al desarrollo normal. Se reanudará las operaciones normales cuando todo vuelva a la normalidad, las cosas a veces no vuelven a la normalidad después de una interrupción de negocio de cualquier magnitud. Ciertamente, las operaciones de negocio se reanudarán, pero algunas cosas pueden cambiar permanentemente como consecuencia de esta interrupción.

Fase de mantenimiento y revisión: Esta fase debe ocurrir independientemente de que active o no su plan. De forma periódica, debe revisar el plan para asegurarse de que aún esté actualizado y sea relevante. A medida que cambian las operaciones y los componentes tecnológicos, a medida que agrega o cambia instalaciones o ubicaciones, el plan debe estar actualizado.

Los planes antiguos son peligrosos porque brindan una falsa sensación de seguridad y pueden generar brechas importantes en la cobertura. Si no se mantiene un plan, también se desperdicia todo el tiempo y el dinero invertidos en la creación del plan. Y en caso de que se active el plan, hay que evaluar la efectividad del plan después, cuando las cosas vuelvan a la normalidad. Revisar el plan inmediatamente después de una interrupción brindará información valiosa sobre lo que funcionó y lo que no funcionó.

Existen otras consideraciones a tomar en cuenta para la implementación de las estrategias de mitigación y son las tareas y los recursos que deben asignarse. Para que no se pase de alto ninguna tarea o recurso, es importante tratar la implementación de la estrategia como un proyecto y en el que serviría desarrollar el EDT (Estructura de Desglose de Trabajo) para desarrollar a partir de este: tareas, recursos y cronogramas. Así se sabrá si algunos recursos se necesita adquirirlos, actualizarlos o instalarlos. A partir de este EDT también se puede hacer la definición de roles y responsabilidades para cada tarea identificada. Como se ha mencionado algunas veces en esta unidad es muy importante que se priorice siempre las actividades o tareas más críticas o importantes necesarias para activar en caso de que se dé la interrupción de los servicios de la organización por alguna anomalía y como en todo proyecto aquí también se puede obtener presupuestos, líneas de tiempo, dependencias y restricciones para las actividades restantes del plan de continuidad.

Para las estrategias de mitigación se puede considerar también recursos como los servicios Cloud o en la Nube, por los que la mayoría de las organizaciones ha optado en usar los últimos años como estrategias de mitigación. Recordemos que estos servicios ofrecen:

- IaaS (infraestructura como servicio)
- PaaS (plataforma como servicio)
- STaaS (almacenamiento como servicio)
- DRaaS (recuperación ante desastres como servicio)
- SaaS (software como servicio)

La computación en la nube permite el uso de recursos informáticos (hardware y software) que se entregan como un servicio a través de una red (normalmente Internet). Las organizaciones generalmente pagan por los servicios en la nube y los usuarios finales acceden a aplicaciones basadas en la nube a través de un navegador Web o una aplicación móvil o de escritorio liviana.

Cuando la organización opta por SaaS, los usuarios tienen acceso a bases de datos y software de aplicación y los proveedores de la nube administran la infraestructura, las plataformas que ejecutan las aplicaciones y todas las operaciones de recuperación de desastres de TI. Esto permite que las organizaciones reasignen los costos de operaciones de TI de los gastos de hardware/software y los gastos de mano de obra asociados con el soporte de TI, hacia el cumplimiento de otros objetivos. También los servicios en la

nube permiten a los usuarios obtener, configurar e implementar servicios en la nube por sí mismos utilizando catálogos de servicios en la nube, sin necesidad de asistencia de TI. Para una conectividad segura, los clientes pueden utilizar el cifrado SSL/TLS a través de Internet o redes privadas virtuales (VPN) dedicadas con cifrado basado en IP.

En el modelo PaaS, los proveedores de la nube ofrecen una plataforma informática completa, que normalmente incluye un sistema operativo, un entorno de ejecución del lenguaje de programación, una base de datos y/o un servidor Web.

Finalmente, para terminar con el desarrollo del plan de continuidad de negocio se hace la debida comunicación, para eso es necesario un plan de comunicación, quienes serán los responsables y cómo y qué herramientas se utilizarán para las mismas. La comunicación debe ser tanto interna como externa. Estos planes de comunicación deberán estar establecidos para, si en caso hay una interrupción, haya un proceso preestablecido para hacer conocer esta situación.

6.2.6. Capacitación, pruebas y revisión del proceso de la continuidad de negocio

La capacitación en recuperación de la continuidad de negocio se debe ver desde dos enfoques. El primer enfoque es tomar en cuenta que al inicio siempre se hace una respuesta física cuando la interrupción se da por un desastre natural, por ejemplo, un terremoto en el que se debe evacuar el edificio. El segundo enfoque de la capacitación tiene que ver con asegurar que los distintos equipos de respuesta sepan cómo implementar el plan de continuidad de negocio y que tengan las habilidades necesarias para hacerlo.

Como toda capacitación existe algunas actividades que realizar como: definir el alcance y los objetivos de la capacitación, realizar una evaluación de las necesidades (análisis de brechas), desarrollar la capacitación, programar e impartir la capacitación y monitorear/medir la capacitación.

Es importante hacer una evaluación de necesidades para saber precisamente qué habilidades y capacidades tiene el personal de la organización y qué recursos disponibles se tienen tanto para la capacitación como para lograr las competencias de lo que se va a enseñar, se considera que la capacitación dirigida para mantener o mejorar las habilidades,

especialmente las relacionadas con las funciones comerciales de misión crítica, se puede lograr con relativa rapidez y, a menudo, a un costo razonable.

Cuando se lleva a cabo la capacitación es importante evaluar si se cumplieron los objetivos y esto se lo hace generando una evaluación que ayude a ver si los dos enfoques de capacitación quedaron claros puede ser por medio de exámenes o demostraciones prácticas.

Las pruebas del plan de continuidad de negocio ayuda a asegurarse de que el plan funcione como se espera en caso de una interrupción, nos ayudan, a comprender de manera más robusta los procesos de la organización, los procedimientos por parte del equipo de implementación del plan, también se tiene más claro si las actividades y tareas son las que previamente se identificó, lo mismo ocurre con los recursos y lo más importante determinar el costo y viabilidad de las estrategias de mitigación propuestas.

Las auditorías del plan de continuidad de negocio implican un conjunto de tareas que ayudan a reducir el riesgo de una intrusión o un ataque. Las auditorías se preocupan principalmente por garantizar que la organización mantenga la confidencialidad, integridad y disponibilidad de los datos, ya que estas son las áreas que suelen ser atacadas. Una auditoría de sistemas de TI generalmente se enfoca en realizar una evaluación sistemática de la seguridad de varios sistemas de TI midiendo qué tan bien se ajusta a los criterios o requisitos establecidos. Incluye una evaluación o revisión de la configuración física y el entorno de la red y los sistemas, la configuración del software, el manejo (almacenamiento, transporte, acceso, etc.) de los datos, los datos sensibles en particular y el acceso de los usuarios. Estas auditorías buscan:

- Asegurar que las estrategias de mitigación de riesgos de TI estén implementadas y correctamente implementadas/configuradas.
- Asegurar que los sistemas identificados por el plan de continuidad de negocio aún estén en su lugar y funcionando.
- Identificar áreas donde se ha implementado nueva tecnología y es posible que no se incorporen al plan de continuidad de negocios.
- Identificar áreas donde la tecnología ha sido retirada o modificada, resultando en la necesidad de revisar el plan continuación de negocio.

- Revisar los procesos identificados en el plan de continuidad de negocio con respecto a los sistemas de TI para garantizar que los pasos y procesos aún sean correctos, completos y relevantes.
- Verificar que el equipo de respuesta a incidentes de TI (CSIRT, CERT o cualquier término que use) está intacto y tiene una comprensión clara de los roles, responsabilidades y cómo implementar los segmentos específicos de TI del plan de continuidad de negocio.

 Estamos finalizando el estudio del contenido planificado para la semana 13 y 14, estará en la capacidad de identificar cómo se lleva a cabo el proceso de gestión de continuidad de negocio, así como conocer cada una de las fases y las actividades que se sugieren para llevar a cabo el desarrollo el plan de continuidad de negocio. Es importante que se apoye con bibliografía complementaria disponible digitalmente para que complete su estudio y se recomienda desarrollar las actividades de aprendizaje recomendadas.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

Lecturas en bibliografía básica, complementaria y recursos educativos abiertos

- Revise la bibliografía complementaria para afianzar los conocimientos estudiados en la semana 13.
- **Libro Gestión de la Seguridad de la Información** (Capítulo 9: Gestión de la continuidad del negocio.)
- **Libro ITIL Information Technology Infrastructure Library** (Capítulo 4: Diseño del Servicio punto 4.7)
- **Libro Business Continuity and Disaster Recovery Planning** (Apéndice A, B, C, D, E, F, G)

- **Actividad 1**

Basándose en la revisión de la bibliografía y recursos educativos abiertos sugeridos para su estudio y los que usted puede adicionar, por favor desarrolle una estrategia de mitigación para tratar Datos críticos en una organización.

- **Actividad 2**

Basándose en las lecturas realizadas respecto al desarrollo del plan de continuidad de servicios de TI, proponga el desarrollo de un plan, identifique las actividades, tareas y recursos necesarios para ese plan, suponiendo que el escenario a cubrir son ataques por DoS a los sistemas críticos de la empresa.

Aunque es muy importante tener un plan de continuidad de negocio, también las organizaciones tienen como pilar fundamental un proceso de gestión de incidentes de seguridad, para el cual crean un equipo y establecer un CSIRT se transforma en un proyecto cuyos objetivos deben estar alineados a los de la organización. En el momento que las organizaciones cuentan con los recursos para crear un CSIRT es que esto se convierte en una ventaja competitiva.



Semana 15

6.3. Gestión de incidentes de seguridad - CSIRT

Los equipos de respuesta a incidentes de seguridad informática (CSIRT) responden a un incidente de seguridad informática cuando surge la necesidad o también se enfocan en la búsqueda de problemas para prevenir. Entonces ¿Qué es un incidente de seguridad? Es un evento albero, real o potencias, que involucra la seguridad de los sistemas de información y sus redes o si se ve afectada o pasada por alto una política de seguridad de forma implícita o explícita.



Es importante recordar el tema de incidentes de seguridad, para profundizar un poco más le invito a revisar la siguiente [matriz de incidentes de seguridad](#), identificados por el equipo de CSIRT del Gobierno de Chile.

Para (Van der Kleij et al., 2017) un beneficio importante de tener un proceso de respuesta a incidentes es que es un proceso sistemático (es decir, siguiendo una metodología consistente de manejo de incidentes). Esto ayuda a maximizar la posibilidad de tomar las acciones apropiadas para manejar el incidente. Además, la capacidad de respuesta a incidentes ayuda a las organizaciones a minimizar las consecuencias de los incidentes.

Los equipos de respuesta a incidentes de seguridad informática (CSIRT) desempeñan un papel importante para responder a los incidentes. Los equipos de respuesta a incidentes se pueden formalizar, de modo que realizar la respuesta a incidentes sea su función principal, es por eso por lo que este equipo por lo general trabaja *ad hoc*, ya que los miembros se reúnen para responder a un incidente cuando surge la necesidad. Los miembros de este equipo son personas con perfiles en TI y son personal de las organizaciones que conforman un equipo CSIRT, una vez que se ha detectado un incidente, uno o más miembros del equipo, según sus roles a cumplir y la magnitud del incidente y la disponibilidad del personal, se encargarán inicialmente del incidente. Lo primero que hace del equipo es analizar los datos del incidente, determinar el impacto del incidente y aplicar las estrategias de continuidad de negocio para limitar el daño y restaurar los servicios normales.

El éxito del CSIRT depende de algunos factores, como los recursos técnicos a su disposición y el nivel de conocimientos y habilidades de los miembros del equipo. Además de estos factores, el éxito de un equipo también depende en gran medida de la participación y cooperación de los miembros individuales del CSIRT y otras personas, equipos y departamentos dentro y fuera de la organización dependencias de la organización. Las amenazas de hoy en día y los tipos de ataques a los sistemas de información de las organizaciones determinan que los equipos de CSIRT trabajen juntos con otros actores, o con otros equipos, una buena práctica entre ellos es que, cuando hay un ataque, existen redes informales de CSIRTS donde se puede consultar y se comparte estrategias de defensa. Ahora bien, la creación de un equipo CSIRT de miembros capacitados no asegura el éxito y que el trabajo en equipo no se produce por casualidad.

6.3.1. Ciclo de respuesta a incidentes

El ciclo de respuesta a incidentes, es una metodología o ciclo, que independientemente del tipo de ataque, propone un conjunto de actividades genéricas tanto para la detección de intrusos como para la respuesta a

incidentes y es vital importancia que el personal o equipo de CSIRT sean expertos en este tema.



En la Unidad 5 punto 5.7 se estudió el Manejo de incidentes informáticos, se recomienda que revise nuevamente este tema.

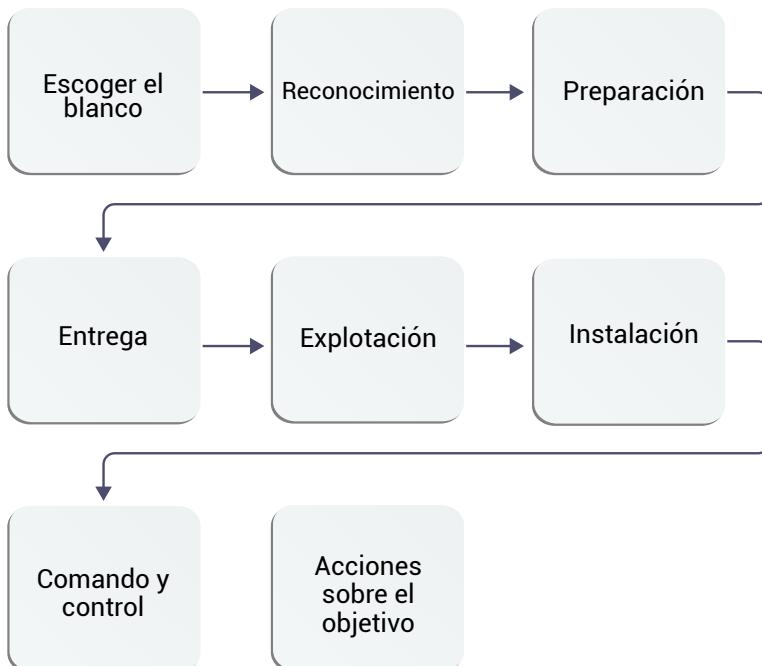
Otra buena práctica para el equipo de CSIRT además de ser expertos en dar respuesta a incidentes, es conocer la manera cómo un atacante opera, para así saber cómo defender los sistemas de TI de su organización. El proceso o modelo más utilizado por los atacantes es el conocido como la Cadena de la Muerte.

6.3.2. Cadena de muerte – Kill Chain

Es una serie de pasos que un atacante debe realizar para lograr un objetivo, ver en la figura 56. Puede ser utilizada por un atacante a sistemas informáticos mediante una red, pero también se puede utilizar para muchas actividades adversas, es un modelo cíclico y no lineal.

Figura 56.

Fases del Kill Chain



Targeting (Escoger el blanco): el atacante identifica su objetivo, esto puede ser por su propia iniciativa o porque alguien o una organización lo solicita o patrocina. El objetivo puede ser una organización, datos, un activo, etc. Esta fase se enfoca en el motivo o lo que le motiva al atacante a buscar su blanco, comprender a donde se dirige le da una idea al equipo defensor de lo que busca el atacante (los objetivos finales del atacante) y puede conducir a mejores técnicas defensivas.

Reconnaissance (Reconocimiento): una vez que el atacante decidió a quién y qué atacar, empieza el reconocimiento, empieza a investigar a indagar y obtener la mayor cantidad de información posible sobre la víctima. El reconocimiento se clasifica según el tipo de datos buscados y los métodos de recopilación. La capacidad del equipo defensor para detectar esta actividad de reconocimiento varía mucho. Los métodos activos son mucho más fáciles de detectar que los métodos pasivos, por ejemplo, el equipo de defensa de una organización tiene más control sobre la información sólida que sobre la información blanda. Por ejemplo, detectar las vulnerabilidades en forma de escaneo de puertos es más fácil que detectar la recopilación pasiva que se hace por parte de un atacante utilizando ingeniería social.

Weaponization (Preparación): el atacante lo que busca es una vulnerabilidad para ser explotada de manera confiable y crear señuelo o un paquete que luego es entregado al objetivo, por ejemplo, un documento malicioso, un script de explotación, etc. El atacante lo que hace es crear *exploit* dirigido al software de la organización que tenga una vulnerabilidad, los sistemas con más vulnerabilidades son aquellos sistemas informáticos que han sido desarrollados con características propias para los procesos críticos de la organización, sin embargo, existen sistemas implementados de casas comerciales conocidas que tienen vulnerabilidades, aunque siempre están desarrollando parches para poderlas resolver. Cada vulnerabilidad parcheada limita un poco a los atacantes y los obliga a encontrar nuevas vulnerabilidades para explotar, pero es un proceso costoso y que requiere mucho tiempo.

Delivery (Entrega): El atacante ha reunido toda la información posible hasta el momento para crear el ataque, ahora está listo para la entrega. Es importante tomar en cuenta en esa fase que solo se debe llevar la carga útil a la víctima. Es considerada la primera fase activa, es decir, el atacante es quién está activo en este proceso. Para (Roberts & Brown, 2016) los escenarios de entrega comunes son:

- **Spear phishing:** El atacante envía comunicaciones directas (a menudo correo electrónico) a un objetivo específico, pero estas comunicaciones en realidad son recursos armados, ya sea como un archivo adjunto o como un enlace. La comunicación generalmente está diseñada para parecer legítima y reducir las sospechas en la mente del usuario objetivo.
- **Inyección SQL:** El atacante envía un comando a una aplicación Web que se pasa al servidor de la base de datos y se interpreta directamente. El atacante tiene la capacidad de ejecutar cualquier comando de la base de datos, incluida la modificación de credenciales, la extracción de información o (en muchos casos) la ejecución de comandos en el sistema operativo host.
- **Compromiso Web estratégico (abrevadero):** El atacante primero compromete un recurso secundario, generalmente un sitio Web y coloca un exploit del navegador en él.

Exploitation (Explotación): La explotación es el punto donde los atacantes obtienen el control de la ejecución del código y comienzan a ejecutar su propio código, pero se da, no solo con la entrega, sino que el objetivo de alguna manera haya dado paso a que esta entrega sea explotada y que el atacante interactúe con el sistema objetivo.

Installation (Instalación): Una vez que los atacantes han ejecutado el código, su primer movimiento suele ser solidificar su punto de apoyo. O en todo caso si quizás se trata de un malware, en esta fase se instala en la máquina. Se trata también de establecer la persistencia en el sistema o red mientras pueda o dure su ataque.

Command and Control (Comando y Control): es la fase donde el atacante tiene ya el control del sistema o proceso de la víctima en donde podrá ya robar información u buscar cumplir sus objetivos, como robar credenciales, información confidencial, instalar programas espías, conocer la red del usuario, etc.

Actions on Objective (Acciones sobre el objetivo): Es la fase donde el atacante no solo obtiene lo que buscaba, sino que quiere o intenta expandir su ataque a más objetivos dentro del sistema o proceso víctima. La Fuerza Aérea de Estados Unidos clasificó algunas acciones dentro de esta fase:

- **Destruir:** la razón del ataque es destruir un elemento físico o virtual, como datos, archivos o bajar un sistema hasta eliminarlo.
- **Denegar:** el atacante hace que un servicio no esté disponible por lo general usando ataques de denegación de servicio que no permiten el acceso a un sitio. Otro ejemplo es el *ransomware*, que cifra los datos de un usuario y requiere el pago antes de que el atacante (en teoría) descifre los datos para volver a utilizarlos.
- **Degradar:** El atacante degrada la utilidad de los recursos alterando los mismos.
- **Interrumpir:** El atacante interrumpe la gestión normal de las actividades y operaciones normales de la organización.
- **Engañar:** El atacante busca hacer que el objetivo crea algo que no es cierto. Por ejemplo el atacante inserta información falsa en un flujo de trabajo para redirigir activos o información.

Hasta el momento conocemos dos maneras de que se puede proceder para obtener un recurso o información de una organización y que el equipo de defensa debe conocer, cómo responder a un incidente como equipo de defensa o como atacar, para poder saber cómo actúa o procede un atacante.

6.3.3. Estableciendo un CSIRT

Existen diferentes tipos de CSIRT, depende mucho del tipo de organización en el que se va a crear el equipo, sin embargo, existen actividades similares que se pueden desarrollar independientemente del tipo de CSIRT al que se refiera.

Antes de describir los pasos más importantes, algunos expertos en materia aconsejan que el establecimiento de un CSIRT sea con base en el ciclo de mejora continua *Ciclo de Deming*, ya que siempre se buscará que este equipo pueda manejar los incidentes de acuerdo con nuevas tecnologías. En el siguiente recurso interactivo se indica las fases principales para establecer un CSIRT.

Fases para establecer un CSIRT

6.4. Buenas prácticas para la continuidad de negocio

Existen algunas normas, marcos de referencia o buenas prácticas que definen la estructura, los pasos y actividades del proceso de continuidad de negocio de una organización, las mismas se describen a continuación:

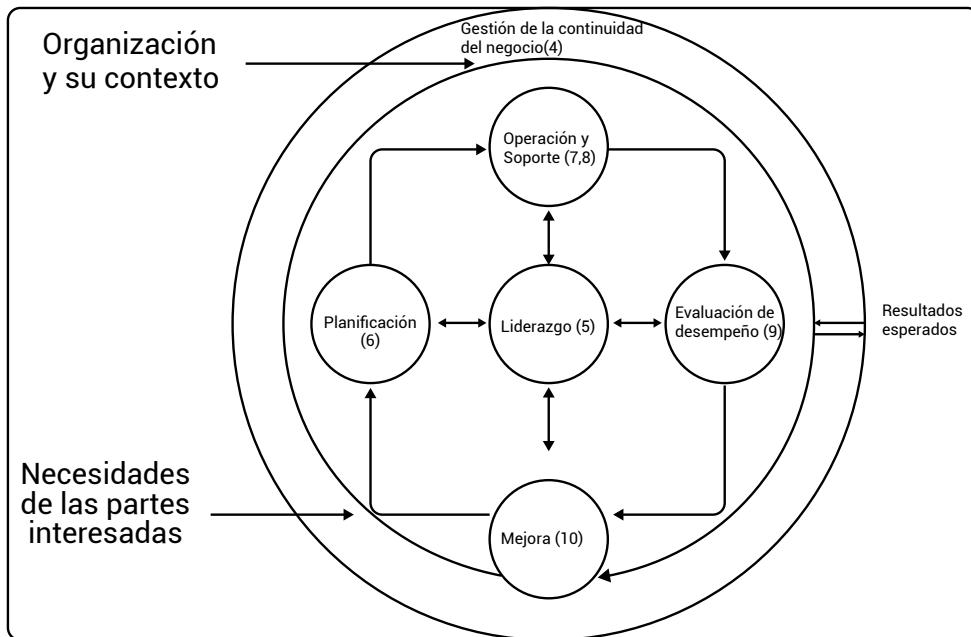
6.4.1. ISO 22301:2019 Gestión de la Continuidad del Negocio

La ISO 22301 es el estándar internacional que ayuda a las organizaciones a implementar planes de continuidad del negocio para protegerlas y ayudarlas a recuperarse de incidentes que interrumpen los sistemas o los procesos críticos de la información, ayudando a identificar las amenazas potenciales para desarrollar la capacidad de hacer frente a eventos imprevistos.

ISO 22301 se basa en la estructura de alto nivel que ayuda a mantener la coherencia, alinea los diferentes estándares del sistema de gestión que se basan en este marco, como todas las ISO, está formada por subcláusulas coincidentes con la estructura de nivel superior y aplica un lenguaje común sobre todo porque se puede combinar con otros estándares. Aplicarlo hace más fácil para las organizaciones incorporar su *Sistema de Gestión de Continuidad del Negocio (SGCN)* en los procesos de negocio centrales o críticos, obtener eficiencias y una mayor participación de la alta dirección.

Al igual que todas las ISO su proceso operativo se basa en el ciclo de Deming que es el ciclo de mejora continua, Planificar-Hacer-Verificar-Actuar (PDCA). Se aplica a todos los procesos y al SGCN en su conjunto para la mejora continua. En la figura 57 se muestra cómo las cláusulas 4 a 10 de ISO 22301 se pueden agrupar en relación con PDCA, obtenido de (BSI GROUP, 2016).

Figura 57.
PDCA de la ISO 22301



Nota. Adaptado de BSI GROUP, 2016.

La organización y su contexto – Necesidades y expectativa de las partes interesadas: Se refiere a conocer la organización, tanto las necesidades internas como externas que son importantes para el SGCN y cómo se relacionan con los resultados esperados. Se identifica las partes interesadas y establecer límites claros para el alcance del sistema de gestión para saber que va a cubrir este sistema y que no.

Liderazgo: La alta dirección debe mostrar su compromiso con el SGCN sobre todo para la asignación de recursos y de procurar alcanzar los objetivos del SGCN por lo que se debe asegurar que el SGCN sea compatible con la estrategia dirección de la organización. Lo que se procura también es mostrar cómo se integran los requisitos de su SGCN en los procesos comerciales de la organización. Es importante que para establecer un SGCN la creación primero de políticas que los respalden y que cumpla con los requisitos legales y requisitos reglamentarios. La alta dirección tiene que hacer el seguimiento para que el ciclo PDCA sea cumplido.

Planificación: se requiere que la organización identifique los riesgos por los que los objetivos estratégicos del SGCN no tendrían éxito. Esto significa

que se debe comprender tanto la cultura interna como el entorno externo en el que opera la organización y también cuáles pueden ser las barreras probables que impidan que estos objetivos se cumplan y en todo caso si se implemente que factores impiden que sea eficaz. Estos objetivos de SGCN deben ser establecidos, medibles e identificar quién estará a cargo de verificar que sean cumplidos.

Soporte y Operación: la cláusula de soporte se trata sobre los recursos que se van a necesitar para establecer, implementar y mantener un efectivo SGCN. El equipo responsable del SGCN deberá tener las capacidades y conocimientos suficientes, también se debe considerar la comunicación de este equipo con todos los interesados y cómo responden estos sobre todo cuando hubiera un incidente. Debe haber una adecuada gestión de documentos del SGCN.

La cláusula de operación se refiere que los procesos sobre todo para gestionar los riesgos del SGCN están funcionando correctamente. Se debe definir el orden y el tiempo de recuperación para las actividades críticas que respaldan los productos y servicios de la organización. Es buscar que los procesos del SGCN se centren en minimizar las consecuencias de una interrupción. También necesitará tener procedimientos documentados para restaurar y devolver las actividades que han sido interrumpidas por un accidente a la normalidad. También tiene que ver con los procesos implementados que ayuden con la mejora continua del SGCN.

Evaluación de desempeño: Incluye el mantenimiento y la evaluación del SGCN por medio de auditorías la organización obtendrá las métricas para verificar si son las adecuadas para el desempeño de la SGCN. En caso de ser necesario se aplica acciones correctivas. La alta dirección también revisa y aprueba estos cambios.

Mejora: Identifica las acciones a tomar para mejorar el rendimiento de un SGCN en el tiempo y se asegurar que sea robusto y también se verifica que se implementen las acciones correctivas derivadas de auditorías, revisiones, prácticas, etc.

6.4.2. ITIL

Information Technology Infrastructure Library (ITIL) es un conjunto de buenas prácticas enfocadas a dar lineamientos para trabajar con infraestructura de las tecnologías de la información. Uno de sus apartados

es *Gestión de la Continuidad del Servicio de TI* (ITSCM) que es dar soporte al proceso de continuidad del negocio sobre todo dando garantía que las instalaciones de TI y servicios puedan volver a la normalidad en un tiempo requerido.

Los objetivos que incluye un ITSCM son los que se muestran en la tabla 33.

Tabla 33.

Objetivos de un ITSCM

Objetivos de un ITSCM
Mantener un conjunto de planes de continuidad y recuperación.
Realizar periódicamente Análisis de Impacto sobre el Negocio (BIA).
Realizar periódicamente estimaciones de riesgo y ejercicios de gestión.
Asesorar y guiar a todas las áreas de negocio y de TI en todos los temas relacionados con la continuidad y la recuperación.
Garantizar que los mecanismos adecuados de continuidad y recuperación están listos para poder cumplir o superar los objetivos particulares de continuidad acordados con el negocio.
Evaluar el impacto de todos los cambios sobre los planes de continuidad y recuperación.
Implementar medidas proactivas para mejorar la disponibilidad de los servicios (cuando sea justificable en costes).
Negociar acuerdos con otros proveedores de servicios de TI en lo relativo a capacidad de recuperación requerida para soportar los planes de continuidad.

Junto con el ciclo de vida del ITSCM se debe haber una gestión adecuada de la información que este ciclo de vida maneja. Para establecer un ITSM se necesita: Planes y estrategias de la organización, Información de las Tecnologías de información que la organización tiene o utiliza, Información financiera, información de cambios, etc. Y como salida del ciclo de vida tendremos: Políticas y estratégicas del ITSCM revisadas, informes de Análisis de impacto y de riesgos, Planes de continuidad de negocio e informes de pruebas.

Las métricas para medir la efectividad del ITSCM según (Van Bon et al., 2017) son:

- Informes de auditorías periódicas de los planes del ITSCM.
- Niveles de acuerdo de servicio.
- Resultados de las pruebas del ITSCM.
- Revisión periódica de los planes de ITSCM.

Los riesgos al implementar un ITSCM es sobre todo la falta de compromiso de la alta dirección, falta de recursos y presupuestos, darles más

importancia a las tecnologías de información que a los procesos y necesidades de la organización de cara a los clientes y no hacer un profundo análisis de riesgos.

6.4.3. COBIT

Objetivos de Control para Información y Tecnologías Relacionadas es un marco de buenas prácticas para la gestión y control de la información en sistemas de TI, este marco se enfoca también en el gobierno de TI, objetivos de control, medidas de desempeño, contingencia, aspectos críticos de éxito y modelos de madurez (Mora Yomayuza, 2018).

COBIT es otra buena práctica que apoya a tener un enfoque adecuado en la creación, desarrollo e implementación de un plan de continuidad sobre todo con su apartado DSS04 “Gestionar la Continuidad” que son objetivos de controles específicos para asegurar la continuidad de negocio y de las operaciones de una organización. Ver en documento Proceso DSS004 Gestionar la Continuidad.

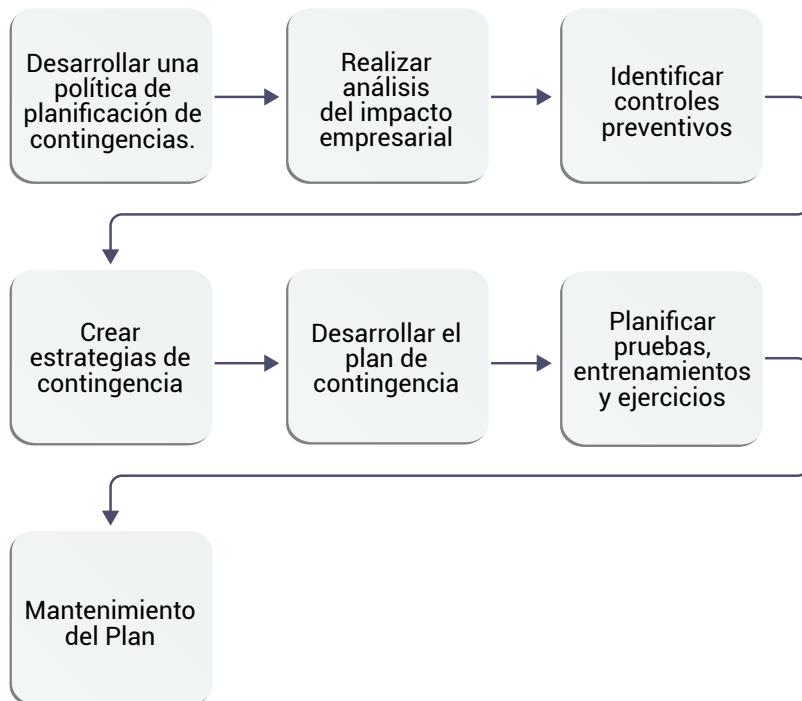
[Proceso DSS004 Gestionar la Continuidad](#)

6.4.4. NIST SP 800-34

El Instituto nacional de Estándares y Tecnologías NIST desarrolló una guía para comprender el propósito, proceso y un formato del desarrollo de planes de contingencia de los sistemas de información a través de directrices y prácticas reales para una organización (Mora Yomayuza, 2018). Lo que propone esta guía es un proceso de planificación de contingencias que se muestra la figura 58.

Figura 58.

Proceso de planificación de contingencias según NIST SP 800-34



La planificación de contingencia se refiere a las medidas provisionales para recuperar servicios del sistema de información después de una interrupción por algún incidente. Por ejemplo, una medida puede ser que se reubiquen los sistemas de información.



Para más información sobre este estándar lo puede revisar [Guía de planificación de contingencias para sistemas de información federal](#).



Al finalizar esta semana estará en capacidad de comprender como se forma un equipo CSIRT y cuáles son las buenas prácticas que las organizaciones pueden utilizar como base para incluir un sistema de continuidad de negocio en una organización. Se recomienda que refuerce conocimientos con las actividades de aprendizaje recomendadas, así como la lectura de algunos recursos.



Actividades de aprendizaje recomendadas

Con la finalidad de que fortalezca sus conocimientos es importante que usted lleve a cabo las siguientes actividades de aprendizaje:

- **Actividad 1**

Una vez que haga la revisión de la bibliografía básica, complementaria y recursos. Desarrolle el siguiente ejercicio: Proponga la creación de un CSIRT para una IES *Institución de Educación Superior*, sobre todo tome en cuenta, los principales ataques o incidentes que sufren las IES y que el equipo CSIRT deberá estar dispuesto a resolver o defender.

- **Actividad 2**

Una vez que haga la revisión de la bibliografía básica, complementaria y recursos. Haga un cuadro comparativo entre las buenas prácticas consideradas para la gestión de continuidad de negocio, sobre todo de las estudiadas en esta unidad.

Una vez que ha estudiado los conceptos relacionados con la unidad que comprende la semana 13 y la semana 14, le invito a desarrollar la Autoevaluación 8 con el fin de evaluar los conocimientos adquiridos hasta el momento.

¡Éxitos en la autoevaluación!



Autoevaluación 6



Una vez que ha estudiado los conceptos relacionados a la unidad que comprende la semana 13 y la semana 14, le invito a desarrollar la autoevaluación 8 con el fin de evaluar los conocimientos adquiridos hasta el momento.

¡Éxitos en la autoevaluación!

1. La gestión de continuidad de negocio es:

- a. La combinación de actividades de prevención de riesgos y de recuperación de desastres.
- b. La combinación de políticas y estándares de gestión de riesgos.
- c. Conjunto de actividades netamente orientadas a tratar los ataques cibernéticos.

2. Determinar la estrategia de continuidad se refiere a:

- a. Identificar las amenazas externas de la organización.
- b. Identificar la capacidad de dar respuesta a un incidente.
- c. Identificar los factores que lo hacen materializarse.

3. Los requisitos funcionales para la continuidad de negocio se refieren a:

- a. Detallan procesos, métodos y recursos que deben estar disponibles durante y después de la interrupción.
- b. Componentes básicos de la organización y cómo se interrelacionan para saber las áreas a priorizar.
- c. Aplicaciones e infraestructura de TI.

4. Las principales amenazas que producen incidentes en la que la mayoría de los casos las organizaciones tienen una gran pérdida de sus activos son:

- a. Amenazas a los TI.
- b. Amenazas ambientales.
- c. Amenazas a los SI.

- 5. Los procesos de misión crítica son:**
 - a. Se pueden recuperar a largo plazo.
 - b. Si son interrumpidos su impacto es a largo plazo.
 - c. Procesos que tienen mayor impacto en las operaciones de la organización.
- 6. Es el tiempo en que un proceso se paraliza antes de que sea puesto en funcionamiento nuevamente.**
 - a. Tiempo máximo tolerable de caída.
 - b. Tiempo de recuperación.
 - c. Tiempo de recuperación del trabajo.
- 7. La probabilidad de que ocurra un evento menor es alta, pero la interrupción asociada es relativamente baja, se refiere a:**
 - a. Interrupción menor.
 - b. Interrupción media.
 - c. Interrupción mayor.
- 8. Cómo se llama el método general que un atacante utiliza para poder acceder a un sistema:**
 - a. Respuesta a incidentes.
 - b. Kill Chain.
 - c. ITIL.
- 9. Para establecer un CSIRT en la organización, es importante:**
 - a. Obtener el apoyo y compromiso de la alta dirección.
 - b. Identificar varios ataques durante varias semanas.
 - c. Que existan sistemas interrumpidos por largo tiempo.

10. La norma que se utiliza para establecer un sistema de gestión de continuidad de negocio es:

- a. ISO 27001.
- b. ISO 31000.
- c. ISO 22301.

Puede verificar las respuestas de esta autoevaluación al final del Texto Guía.

[Ir al solucionario](#)

Si su puntaje no es bueno, es importante que vuelva a revisar los contenidos de la unidad y los recursos de aprendizaje, no olvide que puede interactuar con su tutor por cualquier medio de comunicación que brinda la UTPL para que aclare sus inquietudes.

Estimado estudiante, estamos concluyendo el estudio de esta asignatura, agradecemos su preocupación por la misma y su responsabilidad con la realización de las diferentes actividades de aprendizaje, pues, esto le servirá para desarrollar las competencias para su vida profesional.

¡Felicitaciones!



Actividades de aprendizaje recomendadas

Estimado estudiante, estamos en la semana 16 de estudio de esta asignatura, prácticamente finalizando el ciclo académico y el segundo bimestre, es importante que esta semana usted haga el estudio de las unidades 4, 5 y 6. Así mismo, lea por favor, las siguientes recomendaciones como preparación para la evaluación presencial o virtual:

- Haga una lectura comprensiva de los temas y subtemas estudiados en cada unidad. Puede utilizar algunas herramientas como resaltar, hacer resúmenes, mapas mentales, etc.
- Realice las actividades recomendadas en cada semana, tanto las calificadas como las que están expuestas como apoyo para reforzar conocimientos.
- Vuelva a desarrollar las autoevaluaciones.
- Si tiene alguna inquietud o duda respecto a las actividades práctico-experimentales, actividades de contacto con el docente o las de trabajo autónomo, por favor comuníquese con el tutor en los horarios establecidos o utilice los medios de comunicación antes expuesto.
- Esté atento a alguna comunicación sobre las evaluaciones que hacen desde la UTPL.
- Haga con tiempo algún trámite que necesita como para que pueda presentarse a las evaluaciones.
- Consulte el horario y lugar para rendir la evaluación presencial de la asignatura.

Nota. Conteste las actividades en un cuaderno de apuntes o en un documento de Word en caso de ser necesario.



4. Solucionario

Autoevaluación 1		
Pregunta	Respuesta	Retroalimentación
1	a	La información es un conjunto de datos ordenados y con sentido, que describen a algo o alguien.
2	c	Los elementos de los sistemas de información son: software, hardware, personas, infraestructura, información.
3	b	La información exacta y completa significa que es precisa, es decir, es lo que se necesita y lo que se busca.
4	a	La divulgación es cuando la información es expuesta a personas que no son dueños, y por lo general el objetivo es causar daño.
5	b	Una de las amenazas de TI más conocidas es la negación de servicios conocida como DoS.
6	c	La confidencialidad es la característica que especifica que el personal tiene acceso a información de una organización, sea la información digital o no.
7	b	Una amenaza es cuando un evento se materializa por la existencia de una vulnerabilidad, pueden ser de algunos tipos.
8	c	Un ataque es una amenaza de seguridad de la información, proporcionada tanto por un atacante o hacker como por scripts o programas desarrollados con ese fin.
9	c	La norma para establecer un Sistema de Gestión de la Seguridad de la Información, sin importar el tipo de la organización es la ISO 27001.
10	c	La ISO 27001, al igual que todas las normas ISO están basadas en el ciclo de mejora continua o más conocido como ciclo de Deming.

[Ir a la autoevaluación](#)

Autoevaluación 2		
Pregunta	Respuesta	Retroalimentación
1	a	Los factores internos que deben considerarse dentro del proceso de evaluación de riesgo son las políticas, procedimientos o normas de la organización que previamente han sido establecidas, o si no existen habrá que proponerlas.
2	b	La probabilidad de que ocurra un riesgo significa cuán factible es de que ocurra un evento en el tiempo.
3	a	El impacto cuando se materializa un riesgo significa el daño que hace a la organización a nivel de costos o pérdidas de activos.
4	b	El proceso de identificación de activos es determinar los recursos más importantes o que la organización considera de más valor y que quiere salvaguardar.
5	c	Los activos se pueden valorar por los tres pilares de la seguridad que son: disponibilidad, integridad y confidencialidad.
6	b	La identificación de vulnerabilidades se refiere a identificar los fallos que producen que se materialice la amenaza, sea de sistemas informáticos o de cualquier activo de la organización.
7	a	Cuando decimos que las vulnerabilidades pueden encontrarse en aplicaciones, que existen amenazas a nivel de software.
8	b	Es la actividad de evaluar cuánto afectará a la organización si se materializa una amenaza, se llama identificación del impacto.
9	a	La matriz de riesgos es una herramienta para evaluar o estimar riesgos.
10	c	Cuando contrata la organización un seguro para que la empresa pueda restablecer sus funciones después de un desastre natural, hablamos de que está transfiriendo el riesgo a la organización que le brinda el servicio.

[Ir a la autoevaluación](#)

Autoevaluación 3		
Pregunta	Respuesta	Retroalimentación
1	a	El proceso de extracción de información se realiza en la fase de reconocimiento.
2	a	La fase de exploración busca aprovechar las debilidades del sistema.
3	b	Como se ha mencionado, todos los activos de la organización deben participar en lo relacionado a la seguridad.
4	b	La intercepción está relacionada directamente con la confidencialidad.
5	c	XSS hace referencia a la ejecución de scripts.
6	b	El objetivo principal de los ataques DoS es la interrupción de los servicios del servidor.
7	c	Se considera una herramienta intermedia que ayuda al desarrollo del sistema.
8	c	Se ha colocado un archivo.
9	c	Por su definición suplanta direcciones IP.
10	a	Con este script se ejecutará.

[Ir a la autoevaluación](#)

Autoevaluación 4		
Pregunta	Respuesta	Retroalimentación
1	b	Está relacionado con el acceso y manipulación del sistema.
2	b	Es uno de los principios tratados sobre el diseño.
3	a	Es un requisito sobre el acceso.
4	a	Las herramientas b y c son herramientas de análisis forense.
5	b	Cada tres años se lanza una nueva versión.
6	c	Es una característica del ataque denegación de servicio.
7	b	Es algo que pertenece a la persona que no puede cambiarse por otro.
8	c	Es algo que el usuario en algún momento tendrá por diferente medio.
9	a	Es de conocimiento de la persona que quiere acceder.
10	b	Es una característica del mismo.

[Ir a la autoevaluación](#)

Autoevaluación 5

Pregunta	Respuesta	Retroalimentación
1	a	Pertenece a la categoría de sistemas.
2	c	Se debe realizar un proceso metódico.
3	a	Se lo puede considerar como un tema dentro de la organización.
4	c	El principio de DoS.
5	a	No es necesario pagar para su utilización.
6	b	Se la encuentra en esta categoría.
7	b	Se realiza en esta etapa la evaluación de condiciones.
8	a	Es la fase inicial.
9	b	Está dentro de la explicación de la metodología.
10	a	Está dentro de la explicación de la metodología.

Ir a la
autoevaluación

Autoevaluación 6		
Pregunta	Respuesta	Retroalimentación
1	a	La gestión de continuidad de negocio es la combinación de actividades de prevención de riesgos y de recuperación de desastres.
2	b	Determinar la estrategia de continuidad se refiere a identificar la capacidad de dar respuesta a un incidente.
3	a	Los requisitos funcionales para la continuidad de negocio se refieren a los procesos, métodos y recursos que deben estar disponibles durante y después de la interrupción.
4	b	Las principales amenazas que producen incidentes en que la mayoría de los casos las organizaciones tienen una gran pérdida de sus activos son: amenazas ambientales, puesto que no las podemos controlar o predecir cuándo sucederán.
5	v	Los procesos de misión crítica son procesos que tienen mayor impacto en las operaciones de la organización y por lo general tienen que ver con su cadena de valor al producir un producto o servicio.
6	b	El tiempo de recuperación es el tiempo en que un proceso se paraliza antes de que sea puesto en funcionamiento nuevamente.
7	a	Una interrupción menor es cuando la probabilidad de que ocurra un evento menor es alta, pero la interrupción asociada es relativamente baja, es decir, esta interrupción no afecta la marcha normal de la organización y se puede resolver a largo plazo.
8	b	Kill Chain es conocido como el método general que un atacante utiliza para poder acceder a un sistema, y es importante que los equipos de defensa de los sistemas informáticos de una organización lo conozcan.
9	a	Para establecer un CSIRT en la organización, es importante, obtener el apoyo y compromiso de la alta dirección, es por eso que es el primer paso, sin el compromiso de los directivos, no se puede proceder a la creación de políticas en los que va a respaldarse el equipo CSIRT, y no habrá compromiso del resto del personal de la organización.
10	c	La norma que se utiliza para establecer un sistema de gestión de continuidad de negocio es ISO 22301.

[Ir a la autoevaluación](#)



5. Glosario

ISOTools: Conjunto de herramientas para la Gestión de Gobierno, Riesgo y Cumplimiento.

ISO: Organización Internacional de Normalización, presenta una lista de normas y estándares, se consideran en esta guía aquellas para la gestión de la seguridad de la información, riesgos.

SGSI: Sistema de gestión de la Seguridad de la Información.

TIC: Tecnologías de la información y la comunicación.

Activo: Se considera a todos los componentes dentro de la organización, como documentación física, información, hardware, software, personas, reputación de la empresa, etc.

Hacker: Persona con conocimientos sobre informática que ayuda a detectar fallos de seguridad en sistemas.

Atacante: Persona que se introduce en sistemas informáticos sin el consentimiento de la empresa.

Víctima: Persona/empresa que sufre un ataque informático.

OWASP: Proyecto de código abierto que ayuda a la detección de problemas de seguridad sobre aplicaciones.

DEVOPS: Metodología que involucra al equipo de desarrollo (DEV) y el grupo de operaciones (OPS) en el departamento de TIC.

DEVSECOPS: Integración de la seguridad (SEC) dentro de la metodología DEVOPS.



6. Referencias bibliográficas

6.1. Bibliografía básica

Romero, K. y Jaramillo, D (2021). *Texto Guía Fundamentos y aplicación de seguridad de la información*. Loja, Ecuador, Ediloja.

6.2. Bibliografía Complementaria

Albano, M., Vassilakis, V. G. & Logothetis, M. D. (2019). *Ransomware detection and mitigation using software-defined networking: The case of WannaCry*. *Computers and Electrical Engineering*, 76, 111–121.
[Recuperado de enlace web](#)

Alfaro, J. (2017). *Metodología para la gestión de riesgos de TI basada en COBIT 5*. 173. [Recuperado de enlace web](#)

Andalucía, C. C. (2021). *Cloud Center Andalucía*. [Recuperado de enlace web](#)

Aslan, O. & Samet, R. (2020). *A Comprehensive Review on Malware Detection Approaches*. *IEEE Access*, 8, 6249–6271. [Recuperado de enlace web](#)

Ayers, R., Jansen, W. & Brothers, S. (2014). *Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)*. NIST Special Publication, 1 (1), 85. [Recuperado de enlace web](#)

Arteaga Martínez, M. M. (2017). *Gestión de Riesgos de TI - Notas*.

Cajo, I. M. H., Pucuna, S. Y., Cajo, B. G. H., Coronado, V. M. O. & Orozco, F. V. S. (2018). *Estudio Comparativo De Las Metodologías De Análisis Forense Informático Para La Examinación De Datos En Medios Digitales*. European Scientific Journal, ESJ, 14 (18), 40. [Recuperado de enlace web](#)

Cestari Filho, F., Motta, A. C. & Boca Piccolini, J. D. (2014). ITIL: *Information Technology Infrastructure Library*. *BIT - Numerical Mathematics*, 160, 46–49.

Cert.govt.nz. (2021). *Report an issue relating to COVID-19 vaccine scams or misinformation*. [Recuperado de enlace web](#)

Cibercoders. (2019). *What Hiring Managers Look for in a Full Stack Developer*. [Recuperado de enlace web](#)

Correa, R. A., Higuera, J. R. B., Higuera, J. B., Montalvo, J. A. S., Rubio, M. S., & Alberto Magreñán. (2021). *Hybrid security assessment methodology for Web applications*. *CMES - Computer Modeling in Engineering and Sciences*, 126 (1), 89–124. [Recuperado de enlace web](#)

Cristian, B. (2019). *Seguridad Física*. [Recuperado de enlace web](#)

Johanna Cárdenas Solano, L., Eduardo Becerra Ardila, L., & Ernesto Martínez Ardila, H. (2014). *Gestión de la seguridad de la información*. Red Nacional de Investigación y Educación Del Ecuador REDCEDIA, 1–21. [Recuperado de enlace web](#)

CESICAT. (2015). *Equipo de Respuesta a Incidentes de Seguridad Informática. Portal Web Del CERT de La UNAM*. [Recuperado de enlace web](#)

ECALDIMA. (n.d.). *PLAN DE RESPUESTA DE INCIDENTES*. [Recuperado de enlace web](#)

Ecured. (2018). *Requisitos no funcionales*. [Recuperado de enlace web](#)

Encase. (2018). *Guidance Software/Encase Forensic*. [Recuperado de enlace web](#)

Escuela Europea de Excelencia. (2019). *Listado de amenazas y vulnerabilidades en ISO 27001*. [Recuperado de enlace web](#)

DragonJar. (2021). *OSAM*. [Recuperado de enlace web](#)

Delgado, C. A. A. (2017). Fundamentos de seguridad informática. In Areandina (Issue 2). [Recuperado de enlace web](#)

- Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C. & Saltos-Gómez, J. A. (2018). *La seguridad informática y la seguridad de la información. Polo Del Conocimiento*, 2(12), 145. [Recuperado de enlace web](#)
- Google. (2021). *developers.google.com*. <https://developers.google.com/search/docs/advanced/security/https?hl=es>
- Herrera, S., Figueroa, L., Ghunter, D., Lara, C., Viaña, G., Mendez, A. & Lesca, N. (2019). *Métodos y herramientas para el análisis forense de dispositivos móviles. XXI Workshop de Investigadores En Ciencias de La Computación.*
- INCIBE. (n.d.). *Plan de Contingencia y Continuidad de Negocio*.
- Instituto Nacional de Ciberseguridad INCIBE. (2017). *Plan de Contingencia y de continuidad del negocio. Plan de Contingencia y Continuidad de Negocio*, 1–31. [Recuperado de enlace web](#)
- Interpolados. (2020). *ITIL 4: PRÁCTICAS DE GESTIÓN DE ITIL: GESTIÓN DE ACTIVOS DE TI*. [Recuperado de enlace web](#)
- INGERTEC. (2019). *ISO 27001 AL COMPLETO*. [Recuperado de enlace web](#)
- ISACA. (2013). *COBIT 5 para Riesgos*.
- Guaman, F. & Jaramillo, D. (2018). *Seguridad de la información*. In *Seguridad de la información*. [Recuperado de enlace web](#)
- Landoll, D. J. (2017). *Information Security Policies, Procedures, and Standards: A Practitioner's Reference*. CRC Press
- López Álvarez, D. M. (2020). *Método para el desarrollo de software seguro basado en la ingeniería de software y ciberseguridad*. *INNOVA Research Journal*, 5(3.1), 263–280. [Recuperado de enlace web](#)
- Martínez, Y. & Garzón, J. (2018). *Instructivo - Clasificación de Activos de Información*. 3.
- Merino, C., & Cañizares, R. (2011). *Implantación de un Sistema de Gestión de la Seguridad de la Información según ISO 27001*. FUNDACIÓN CONFEMETAL.

MaquinasVirtuales. (2021). *DevSecOps: Seguridad en el Cloud Computing*. Recuperado de enlace web

Merino, C. & Cañizares, R. (2014). *Auditoría de Sistemas de Gestión de la Seguridad de la Información*. Recuperado de enlace web

McGraw, G., Chess, B. & Miques, S. (2011). *Building security In maturity model*. 2012 Faulkner Information Services, May, 1–61. Recuperado de enlace web

MOBILedit. (2020). *MOBILedit*. Recuperado de enlace web

Montaña, O. (2016). *Síntesis OWASP Gestión de Riesgos de la Seguridad en Aplicaciones*.

NETSECURE. (2018). *20 controles Ciberseguridad NIST*. Recuperado de enlace web

Narayan Dash, S. (2020). *MPUG - Where Project Managers and Microsoft Meet*. A Deep Dive into Risk Matrix Reporting. Recuperado de enlace web

Oxygen Forensics, I. (2021). *Oxygen Forensics*. Recuperado de enlace web

Palos, J. (2016). *Manejo de Errores Usando Excepciones Java*. Recuperado de enlace web.

Pastorino, C. (2019). *Técnicas y herramientas OSINT para la investigación en Internet*. Recuperado de enlace web

Pichincha, B. del. (2021). *Backdoor-virus*. Recuperado de enlace web

PNGEGG. (n.d.). *Data Center*. www...

Pressman, R. (2010). *Ingeniería del Software, un enfoque práctico* (M. Hill (ed.); Septima).

REDCEDIA. (2014). *Gestión del riesgo de las TI NTC 27005*.

RITTAL. (2018). *Principales riesgos y amenazas de seguridad IT*. Recuperado de enlace web

Roberts, S. J. & Brown, R. (2016). *Intelligence-driven incident response : outwitting the adversary.*

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, Á. L. & Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades. In Introducción a la seguridad informática y el análisis de vulnerabilidades.* Recuperado de [enlace web](#).

SDK, A. (2019). *Android.* Recuperado de enlace web

SEI. (2021). *The Current State of DevSecOps Metrics.* Recuperado de enlace web

Snedaker, S. & Rima, C. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals.*

SISTESEG. (2018). *Metodología de análisis de riesgo según ISO 27005 : 2018 e ISO 31000 : 2018.*

SISTEL. (2020). *LOS 6 OBJETIVOS BÁSICOS EN LA SEGURIDAD DE LA INFORMACIÓN.* Recuperado de enlace web.

Yenisel, I., Hernández, M., Ailec, D., Dihigo, G. & Cintra, A. V. (2019). *Los requisitos no funcionales de software. Una estrategia para su desarrollo en el Centro de Informática Médica.* Revista Cubana de Ciencias Informáticas, 13(2), 77-90.

Van Bon, J., De Jong, A., Kolthof, A., Pieper, M., Tjassing, R., Van der Veen, A. & Verheijen, T. (2017). *Guía de Gestión - Diseño de Servicio basada en ITIL V3.* Van Haren.

Van der Kleij, R., Kleinhuis, G. & Young, H. (2017). *Computer security incident response team effectiveness: A needs assessment.* Frontiers in Psychology, 8(DEC), 1–8. Recuperado de enlace web.

Valencia-Duque, F. J. & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, 22, 73–88. Recuperado de enlace web.

Zator. (2016). *Curso C++*. Recuperado de enlace web

Recursos Educativos Abiertos (REA)

Título del REA	URL de acceso
Seguridad en sistemas informáticos	Enlace: http://ocw.uv.es/ingenieria-y-arquitectura/seguridad/Course_listing
Seguridad en redes	Enlace web
Criptografía y seguridad informática	Enlace web
Seguridad informática y competencias profesionales	Enlace web
Garantía y seguridad en sistemas y redes	Enlace web



7. Anexos

Procesos Catalizadores COBIT 5

Procesos de Gobierno de TI Empresarial

Evaluar, Orientar y Supervisar

EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno

EDM02 Asegurar la Entrega de Beneficios

EDM03 Asegurar la Optimización del Riesgo

EDM04 Asegurar la Optimización de los Recursos

EDM05 Asegurar la Transparencia hacia las Partes Interesadas

Alinear, Planificar y Organizar

AP001 Gestionar el Marco de Gestión de TI

AP002 Gestionar la Estrategia

AP003 Administrar la Arquitectura Empresarial

AP004 Gestionar la Innovación

AP005 Gestionar la Cartera

AP006 Gestionar el Presupuesto y los Costes

AP007 Gestionar los Recursos Humanos

AP008 Gestionar las Relaciones

AP009 Gestionar los Acuerdos de Servicio

AP010 Gestionar los Proveedores

AP011 Gestionar la Calidad

AP012 Gestionar el Riesgo

AP013 Gestionar la Seguridad

Supervisar, Evaluar y Valorar

MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad

MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno

MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

Construir, Adquirir e Implementar

BAI01 Gestionar los Programas y Proyectos

BAI02 Gestionar la Definición de Requisitos

BAI03 Gestionar la Identificación y la Construcción de Soluciones

BAI04 Gestionar la Disponibilidad y la Capacidad

BAI05 Gestionar la Habilización del Cambio Organizativo

BAI06 Gestionar los Cambios

BAI07 Gestionar la Aceptación del Cambio y de la Transición

BAI08 Gestionar el Conocimiento

BAI09 Gestionar los Activos

BAI10 Gestionar la Configuración

Entregar, dar Servicio y Soporte

DSS01 Gestionar las Operaciones

DSS02 Gestionar las Peticiones y los Incidentes del Servicio

DSS03 Gestionar los Problemas

DSS04 Gestionar la Continuidad

DSS05 Gestionar los Servicios de Seguridad

DSS06 Gestionar los Controles de los Procesos de la Empresa

Procesos para la Gestión de la TI Empresarial

Nota. Tomado de ISACA, 2012, COBIT 5.



Ejemplo de tratamiento de riesgo

Riesgos	Recomendaciones de control	Priorización de las acciones	Selección de control	Recursos	Responsable	Control de tiempo	Comentarios
Acceso lógico no autorizado	<ol style="list-style-type: none"> Control de autenticación de usuario para conexiones externas. Control de gestión de privilegios. Control de gestión de contraseñas para usuarios. Control de uso de contraseñas. Control de políticas de uso de los servicios de red. Control de protección de los puertos de configuración y diagnósticos remoto. Control de identificación y autenticación de usuarios. Control de sistema de gestión de contraseñas. Control para trabajo remoto. 	Muy alta	<ol style="list-style-type: none"> Control de autenticación de usuario para conexiones externas. Control de gestión de privilegios. Control de gestión de contraseñas para usuarios. Control de uso de contraseñas. Control de políticas de uso de los servicios de red. Control de protección de los puertos de configuración y diagnósticos remoto. 	<p>El servidor debe estar bien configurado con cortafuego a nivel físico.</p> <p>y lógico, con antivirus actualizado y bien configurado, protección de los puertos de configuración y diagnósticos remoto.</p> <p>controles a los perfiles de usuarios administradores.</p>	<p>Administrador del servidor</p> <p>Administrador de red</p> <p>Líder de seguridad</p> <p>tecnológica</p> <p>Director de TI</p>	<ol style="list-style-type: none"> Diario Diario Diario 	<p>Controles seleccionados</p> <ol style="list-style-type: none"> Se deben utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios. Se debe restringir y controlar la asignación y uso de los privilegios de las cuentas de usuarios. Se debe controlar la configuración y el acceso físico y lógico a los puertos de configuración y diagnóstico. <p>Protección lógica. Los puertos físicos deben ser protegidos con una contraseña de acceso para cuando se ingrese a los elementos de red por consola y puertos com o serial. Protección física. Solo personal autorizado por el jefe de la unidad de infraestructura podrá entrar directamente a los puertos de configuración en caso de fallas en los equipos. Para aquellos que se encuentran bajo contrato externo, deben ser solicitada la intervención a la mesa de ayuda.</p>

Nota. Arteaga Martínez, M. M., 2017, Gestión de Riesgos de TI - Notas.



Pila de desarrollo completa



Nota. [Adaptado](#) de Cibercoders, 2019.



Ejemplos de los ataques SQL

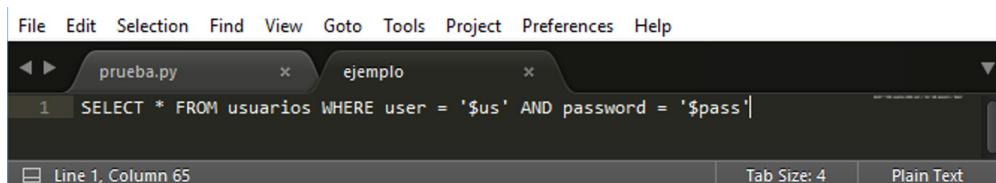
Ejemplos

La consulta mostrada en la Figura 1 muestra el código SQL original que se utilizaría para validación de una entrada:

Ejemplo 1

Figura 59.

Sentencia original a tratar



```
File Edit Selection Find View Goto Tools Project Preferences Help
prueba.py * ejemplo *
1 SELECT * FROM usuarios WHERE user = '$us' AND password = '$pass'
Line 1, Column 65 Tab Size: 4 Plain Text
```

Nota. Elaborado por el autor.

Esperamos se cumpla una sentencia como la siguiente:

parámetros **us**: carlo187 **pass**: L@Kers34S

El resultado se muestra en la figura 2:

Figura 60.

Ejecución de la sentencia resolviendo los parámetros enviados



```
prueba.py * ejemplo *
1 SELECT * FROM usuarios WHERE user = 'carlo187' AND password = 'L@Kers34S'
Line 1, Column 74 Tab Size: 4 Plain Text
```

Nota. Elaborado por el autor.

Consulta que se enviaría a la base de datos para su validación; y, evaluando la misma, permitiría el acceso al usuario en caso de que los datos sean correctos.

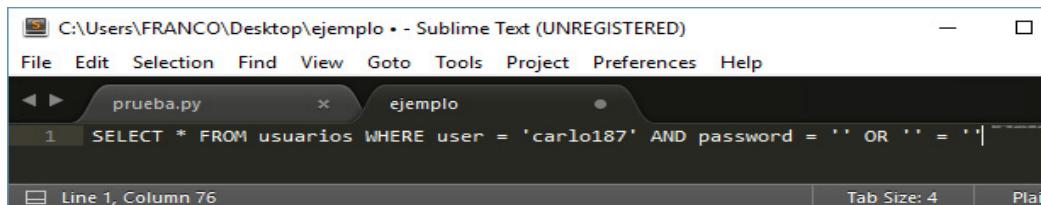
Como se realiza el proceso de Inyección SQL, a continuación, presentamos algunas cadenas para realizar el proceso de violentar esta validación y obtener una respuesta favorable desde la base de datos:

Parámetros: **Us**: carlo187 **Pass**: ' OR " = '

Generando la sentencia así:

Figura 61.

Ejecución de sentencia con aplicación de inyección SQL



A screenshot of the Sublime Text editor. The title bar says "C:\Users\FRANCO\Desktop\ejemplo • - Sublime Text (UNREGISTERED)". The menu bar includes File, Edit, Selection, Find, View, Goto, Tools, Project, Preferences, and Help. There are two tabs: "prueba.py" and "ejemplo". The "ejemplo" tab is active and contains the following SQL query: "SELECT * FROM usuarios WHERE user = 'carlo187' AND password = '' OR '' = ''". The status bar at the bottom shows "Line 1, Column 76", "Tab Size: 4", and "Plain Text".

Nota. Elaborado por el autor.

Según el álgebra relacional, la igualdad siempre devuelve true ($1=1$) es así que si colocamos " $=$ " (vacío es igual a vacío) pasaremos el mecanismo de validación únicamente con el usuario, sin la necesidad de tener la clave, recordar que muchas de las veces el usuario es el correo electrónico o el número de cédula de una persona que es muy fácil de obtener.

Otros posibles valores que validarían la expresión serían:

Ejemplo 2.

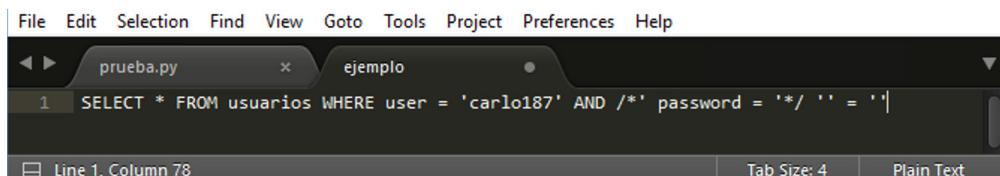
Us : carlo187' AND /*

Pass : */ " = '

Dando como resultado la siguiente expresión:

Figura 62.

Ejecución de sentencia con variación de la aplicación de inyección SQL



A screenshot of the Sublime Text editor. The title bar, menu bar, and tabs are identical to Figure 61. The "ejemplo" tab contains the modified SQL query: "SELECT * FROM usuarios WHERE user = 'carlo187' AND /*' password = '*/ '' = ''". The status bar at the bottom shows "Line 1, Column 78", "Tab Size: 4", and "Plain Text".

Nota. Elaborado por el autor

O en el caso de desconocer tanto el usuario como la clave:

Ejemplo 3

Us : ' OR 1 = 1 -- Lo que generaría la consulta

Figura 63.

Ejecución de sentencia con variación de aplicación de inyección SQL

A screenshot of a terminal window titled "ejemplo". The command entered is:

```
1 SELECT * FROM usuarios WHERE user = '' OR 1 = 1 -- AND password = '$pass'
```

The terminal shows "Line 1, Column 74" and has tabs for "Tab Size: 4" and "Plain Text".

Nota. Elaborado por el autor

Consultas UNION (Union query). En este tipo de ataque se inyectan parámetros destinados a cambiar la salida producida por una consulta determinada. Su objetivo es engañar a la base de datos logrando una respuesta diferente a la esperada por el desarrollador. Para ello se basa en el formato: <consulta original> UNION SELECT <parte de consulta inyectada>, donde la consulta después de la palabra clave UNION está totalmente bajo el control del atacante para que pueda recuperar datos de cualquier tabla que podría no estar prevista en la consulta real. Por ejemplo:

Ejemplo 4

```
User' UNION SELECT cardNumber FROM Creditdetails WHERE  
acctNo=20032 --"
```

Consulta resultante:

Figura 64.

Ejecución de sentencia inyección SQL aplicando Unión

A screenshot of a terminal window titled "ejemplo". The command entered is:

```
1 SELECT id FROM employee WHERE user='' UNION SELECT cardNumber FROM Creditdetails  
WHERE acctNo=20032 --' AND pwd='';
```

The terminal shows "Line 1, Column 116" and has tabs for "Tab Size: 4" and "Plain Text".

Nota. Elaborado por el autor

En este caso la primera consulta dará una respuesta nula o vacía, pero la segunda consulta en cambio devolverá a la aplicación el número de la tarjeta de crédito de la tabla *Creditdetails* que corresponde al parámetro solicitado.

Proceso DSS004 Gestionar la Continuidad

DSS04 Gestionar la Continuidad

Área: Gestión

Dominio: Entrega, Servicio y Soporte

Descripción del Proceso

Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.

Declaración del Propósito del Proceso

Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la empresa ante el evento de una interrupción significativa.

El proceso apoya la consecución de un conjunto de principales metas TI:

Meta TI	Métricas Relacionadas
04 Riesgos de negocio relacionados con las TI gestionados.	<ul style="list-style-type: none">▪ Porcentaje de procesos de negocio críticos, servicios TI y programas de negocio habilitados por las TI cubiertos por evaluaciones de riesgos.▪ Número de incidentes significativos relacionados con las TI que no fueron identificados en la evaluación de riesgos.▪ Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI.▪ Frecuencia de actualización del perfil de riesgo.
07 Entrega de servicios TI de acuerdo a los requisitos del negocio.	<ul style="list-style-type: none">▪ Número de interrupciones del negocio debidas a incidentes en el servicio de TI▪ Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados▪ Porcentaje de usuarios satisfechos con la calidad de los servicios de TI entregados
14 Disponibilidad de información útil y relevante para la toma de decisiones.	<ul style="list-style-type: none">▪ Nivel de satisfacción de los usuarios del negocio y puntualidad (o disponibilidad) de la información de gestión.▪ Número de incidentes en los procesos de negocio causados por la indisponibilidad de la información.▪ Relación o cantidad de decisiones de negocio erróneas en las que la falta de información o la información errónea ha sido la principal causa

Objetivos y Métricas del Proceso

Meta del Proceso	Métricas Relacionadas
4. La información crítica para el negocio está disponible para el negocio en línea con los niveles de servicio mínimos requeridos	<ul style="list-style-type: none">▪ Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento.▪ Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo.▪ Porcentaje de medios de respaldo transferidos y almacenados de forma segura.

5. Los servicios críticos tienen suficiente resiliencia.	<ul style="list-style-type: none">▪ Número de sistemas críticos para el negocio no cubiertos por el plan
6. Las pruebas de continuidad del servicio han verificado la efectividad del plan.	<ul style="list-style-type: none">▪ Número de ejercicios y pruebas que han conseguido los objetivos de recuperación.▪ Frecuencia de las pruebas.
7. Un plan de continuidad actualizado refleja los requisitos de negocio actuales.	<ul style="list-style-type: none">▪ Porcentaje de mejoras acordadas que han sido reflejadas en el plan.▪ Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan.
8. Las partes interesadas internas y externas han sido formadas en el plan de continuidad.	<ul style="list-style-type: none">▪ Porcentaje de interesados internos y externos que han recibido formación.▪ Porcentaje de asuntos identificados que se han tratado subsecuentemente en los materiales de formación.

Nota. Tomado de ISACA, 2012.