SISTEMAS DE PREVENCIÓN DE INTRUSOS (IDS)
EN LA GESTIÓN DE LA INFORMACIÓN

Autores
Cesar Alejandro Vallejo de la Torre
Patricia María Marcillo Sánchez
Martha Viviana Uvidia Vélez

CIDE Editorial

ISBN: 978-9942-792-39-6

César Alejandro Vallejo de la Torre
Patricia María Marcillo Sánchez
Martha Viviana Uvidia Vélez

SISTEMAS DE PREVENCIÓN DE INTRUSOS (IDS) EN LA GESTIÓN DE LA INFORMACIÓN

INTRUSION PREVENTION SYSTEMS (IDS) IN INFORMATION MANAGEMENT

César Alejandro Vallejo de la Torre
Patricia María Marcillo Sánchez
Martha Viviana Uvidia Vélez

Sistemas de Prevención de Intrusos (IDS) en la Gestión de la Información

Intrusion Prevention Systems (IDS) in Information Management

Primera Edición, septiembre 2018

ISBN: 978-9942-792-39-6 (eBook)

CIDEPRO Editorial
Isaías Chopitea y Juan X Marcos
Babahoyo, Ecuador
Móvil - (WhatsApp): (+593) 9 8 52-92-824
www.cidepro.org
E-mail: editorial@cidepro.org

Este texto ha sido sometido a un proceso de evaluación por pares externos con base en la normativa editorial de CIDEPRO.

Diseño y diagramación:
CIDEPRO Editorial

Diseño, montaje y producción editorial:
CIDEPRO Editorial

Hecho en Ecuador
Made in Ecuador

ÍNDICE

PREFACIO

Ante el creciente uso de la web y por ende de los negocios digitales, en la actualidad es común observar como gran parte de compañías y organizaciones consienten a sus socios y usuarios acceder a sus sistemas de información sin ningún tipo de restricción. Pero es de suma importancia saber identificar que recursos de la compañía pueden ser expuestos a los usuarios y cuáles deberían ser absolutamente restringidos con la finalidad de controlar el acceso a los sistemas de información y mantener a buen recaudo los datos de la institución y de los usuarios. Dichos procedimientos deberían ser aplicados de igual forma cuando es permitido el acceso a los sistemas de información de la institución a través de la web.

Además, debido al estilo de vida sencillo que ofrece en la actualidad la tecnología, es común que empleados y administradores de las instituciones puedan acceder a los sistemas de información sin ningún inconveniente desde casi cualquier parte en donde se encuentren, exponiendo la información a que llegue a manos de terceros.

Generalmente los riesgos en términos de seguridad son representados de la siguiente forma:

Riesgo = Amenazas x Vulnerabilidades dividido para las contramedidas.

Donde, las Amenazas simbolizan el tipo de acción o acciones que tienden a ser dañinas, mientras que las vulnerabilidades o falencias simbolizan el nivel de exposición a las amenazas en un escenario particular. Finalmente, las contramedidas simbolizan a las acciones o conjunto de acciones que son implementadas con la finalidad de prevenir las amenazas.

Se debe tener en consideración que las contramedidas que implantemos no deben ser soluciones únicamente técnicas, sino que además deben reflejar la debida capacitación, toma de conciencia y acato de lineamientos estrictamente definidos dirigidos a los usuarios.

En concreto, para que un sistema de información sea totalmente seguro, es necesario identificar las amenazas potenciales y por ende conocer y predecir la trayectoria de ataque de los intrusos. Por tal motivo la intención de este documento es proporcionar una vista general de las posibles motivaciones y métodos de ataques utilizados por hackers y personas mal intencionadas mediante un escenario que permita tener una idea clara de la forma como estos actúan y conocer además métodos y formas para la reducción de riesgos de intrusiones.

PREFACE

In view of the growing use of the web and therefore of digital businesses, it is now common to see how a large number of companies and organizations consent their members and users to access their information systems without any type of restriction. But it is very important to know which company resources can be exposed to users and which should be absolutely restricted in order to control access to information systems and keep the data of the institution and users safe. These procedures should be applied in the same way when access to the institution's information systems is allowed through the web.

In addition, due to the simple lifestyle that technology currently offers, it is common for employees and administrators of the institutions to access information systems without any inconvenience from almost anywhere they are, exposing the information they receive. at the hands of third parties.

Generally the risks in terms of security are represented as follows:
Risk = Threats x Vulnerabilities divided for countermeasures

Where, the Threats symbolize the type of action or actions that tend to be harmful, while the vulnerabilities or flaws symbolize the level of exposure to threats in a particular scenario. Finally, the countermeasures symbolize the actions or set of actions that are implemented in order to prevent threats.

It must be borne in mind that the countermeasures that we implement

should not be solely technical solutions, but should also reflect the proper training, awareness and adherence to strictly defined guidelines for users.

In particular, for an information system to be completely secure, it is necessary to identify potential threats and therefore know and predict the attack path of intruders. For this reason the intention of this document is to provide an overview of the possible motivations and methods of attacks used by hackers and malicious people through a scenario that allows to have a clear idea of how they act and also know methods and ways to the reduction of intrusion risks.

¿QUÉ SON LOS ATAQUES INFORMÁTICOS?

Capítulo 1

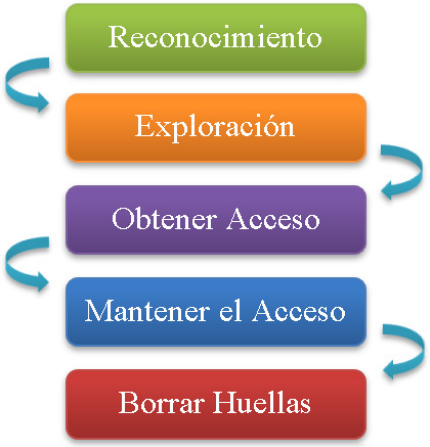
¿QUÉ SON LOS ATAQUES INFORMÁTICOS?

Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización. Para minimizar el impacto negativo provocado por ataques, existen procedimientos y mejores prácticas que facilitan la lucha contra las actividades delictivas y reducen notablemente el campo de acción de los ataques. Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas. (Mieres, 2015)

Anatomía de un ataque informático

Conocer las diferentes etapas que conforman un ataque informático brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional de seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque. La siguiente imagen muestra las cinco etapas por las cuales suele pasar un ataque informático al momento de ser ejecutado: (Mieres, 2015)

Figura 1. Esquema de un ataque informático



Realizado por: Los autores

Etapa 1: Reconocimiento

Reconnaissance (Reconocimiento). Esta etapa involucra la obtención de información (Information Gathering) con respecto a una potencial víctima que puede ser una persona u organización. Por lo general, durante esta fase se recurre a diferentes recursos de Internet como Google, entre tantos otros, para recolectar datos del objetivo. Algunas de las técnicas utilizadas en este primer paso son la Ingeniería Social, el Dumpster Diving, el sniffing. (Mieres, 2015)

Etapa 2: Exploración

Scanning (Exploración). En esta segunda etapa se utiliza la información obtenida en la fase 1 para sondear el blanco y tratar de obtener información sobre el sistema víctima como direcciones IP, nombres de host, datos de autenticación, entre otros. Entre las herramientas

que un atacante puede emplear durante la exploración se encuentra el network mappers, port mappers, network scanners, port scanners, y vulnerability scanners. (Mieres, 2015)

Etapa 3: Obtener acceso

Gaining Access (Obtener acceso). En esta instancia comienza a materializarse el ataque a través de la explotación de las vulnerabilidades y defectos del sistema (Flaw exploitation) descubiertos durante las fases de reconocimiento y exploración. Algunas de las técnicas que el atacante puede utilizar son ataques de Buffer Overflow, de Denial of Service (DoS), Distributed Denial of Service (DDos), Password filtering y Session hijacking. (Mieres, 2015)

Etapa 4: Mantener el acceso

Maintaining Access (Mantener el acceso). Una vez que el atacante ha conseguido acceder al sistema, buscará implantar herramientas que le permitan volver a acceder en el futuro desde cualquier lugar donde tenga acceso a Internet. Para ello, suelen recurrir a utilidades backdoors, rootkits y troyanos. (Mieres, 2015)

Etapa 5: Borrar Huellas

Covering Tracks (Borrar huellas). Una vez que el atacante logró obtener y mantener el acceso al sistema, intentará borrar todas las huellas que fue dejando durante la intrusión para evitar ser detectado por el profesional de seguridad o los administradores de la red. En consecuencia, buscará eliminar los archivos de registro (log) o alarmas del Sistema de Detección de Intrusos (IDS). (Mieres, 2015)

Los riesgos Informáticos

El reporte titulado Data Loss Prevention Best Practices, Managing Sensitive Data in the Enterprise, de Bradley R. Hunter define algunas de las mejores prácticas que pueden aplicar las empresas para prevenir las pérdidas de la información, asegurar el cumplimiento y proteger el valor y la reputación de su marca, dicho reporte es elaborado por Iron Port Systems.

La prevención de la pérdida de la información (DLP, Data Loss Prevention, por sus siglas en inglés) es un serio problema para las instituciones: La cantidad de incidentes y costos relacionados continúan aumentando. Puede tratarse de un ataque malintencionado o un error involuntario, pero la pérdida de información puede afectar la marca, disminuir el valor de todas las partes involucradas y dañar el buen nombre y la reputación de una institución.

La gran mayoría de medios de transmisión electrónica, como los correos electrónicos, mensajes instantáneos, webmails, formatos en sitios web o transferencias de archivos que utiliza una empresa no están sujetos a un control o monitoreo, por lo tanto, siempre existe el riesgo de que la información confidencial caiga en las manos equivocadas. En todos los protocolos básicos de cualquier empresa siempre se debe incluir una solución inteligente y de alto rendimiento.

Los líderes deben buscar proveedores con gran experiencia y conocimientos en el escaneo de contenido para seleccionar la mejor

solución disponible. (Bermeo, 2012)

Protección contra delitos informáticos

Existen protecciones privativas y no privativas. Dentro de las segundas se encuentra la Protección Penal, que trata de aplicar a la materia las normas sobre la violación de secretos de empresas, secreto profesional y corrupción administrativa, y la protección civil que se puede dar en el marco de un contrato o en el plano extracontractual que incluye responsabilidad civil, la concurrencia desleal y el enriquecimiento sin causa. La privativa se da mediante un mecanismo sui géneris de protección, como lo es el derecho de propiedad intelectual, ya sea por la vía de derecho de autor o de Propiedad Industrial. (EcuRed, 2015)

La importancia de la seguridad de la información en las instituciones

El activo más importante en toda organización o institución es la información ya que de ella depende el correcto funcionamiento de las actividades y procesos que se realizan internamente en la institución, este grado de importancia aumenta considerablemente si nos referimos a empresas con automatizaciones altamente calificadas. Ante lo detallado anteriormente, la seguridad de la información sigue siendo el principal factor de riesgo en las organizaciones ya que de esta depende su éxito o fracaso.

De acuerdo al estudio CSI/FBI año 2005 realizado por el Instituto de Seguridad en Computación con la participación de la Agencia Federal de San Francisco, escogiendo una muestra de 700 empresas de

Estados Unidos, las cuales revelaron sus pérdidas causadas por el tipo de amenaza de computadoras, las pérdidas totales para el año 2005 eran de $130, 104,542 para las 700 empresas que respondieron a este estudio, afirmando que las mayores pérdidas se presentan por virus informáticos, acceso no autorizados y el robo de la información, en comparación a los demás problemas que presentan las organizaciones, se sospecha que el aumento en estas tres amenazas podría ser efecto del abuso y uso indiscriminado del internet por parte de los integrantes de la empresa. (Hernández, 2006)

Es de vital importancia considerar que por más de que nuestra institución desde nuestro punto de vista informático sea la más segura, ante el aumento de nuevas tecnologías proporcionadas para manipular la información se han generado un gran número de amenazas dirigidas a atentar la integridad y fidelidad de la información.

El valor y costo de la información para las instituciones

La información en toda organización sea pública o privada, representa un activo estratégico para el correcto funcionamiento y éxito de la misma, por ende, no posee un valor especifico, ya que su importancia es determinada por quienes la manipulan y desde el punto de vista de la institución.

La información se convierte en un activo intangible que puede afectar al negocio, a diferencia de otros recursos como el dinero o el personal de trabajo, la información es susceptible a alteraciones que pueden

llevar al fracaso de la institución, por ello en ocasiones es preferible mantener en secreto el valor de esta.

Si bien, un ordenador nos ayuda al momento de manipular datos e información, pero es importante también que nosotros evaluemos la información y tomemos nuestras propias decisiones tales como revisiones en listas de precios, planificaciones en el lanzamiento de un nuevo producto, entre otros.

La oportunidad, la precisión y la presentación de la información son factores que pueden incidir en el valor de la información, ya que al momento de nivelar estas necesidades se desarrollan retos para el personal que manipula la información, como determinar qué almacenar y qué descartar, hallar mecanismos que permitan organizar la información y restringir el acceso a la misma.

Asignarle valor a la información es un proceso complejo de definir, ya que su valor depende de su complejidad y mientras más detallada se encuentre, su valor aumentará. Por tanto, la información para las empresas, instituciones u organizaciones es un aspecto determinante al momento de tomar decisiones ya que pueden afectar o no la rentabilidad de la institución, por lo que esta debe ser confiable, íntegra y segura, en conclusión, debe integrar estos aspectos de seguridad para garantizar los objetivos de la institución.

Análisis del objetivo de la seguridad informática

Para el análisis de la seguridad informática es preciso conocer de antemano las características de lo que pretendemos proteger, la información.

De esta forma definimos a los *Datos* como la unidad mínima de información, la misma que puede ser una letra o cualquier carácter especial.

A la *Información* como el conjunto de datos que tienen un significado especifico y sentido común por quien lo procesa.

Determinar el valor de la información resulta totalmente relativo, ya que es un recurso que en determinados casos no es valorado adecuadamente por su intangibilidad, escenario que no ocurre con las aplicaciones y equipos informáticos.

Hay información que puede ser perceptible, es decir visualizada por cualquier persona, por ejemplo, el índice de migración de un país; como también hay información que es totalmente privada que solo puede ser visualizada por personal autorizado o por quienes trabajan con ella, por ejemplo, los antecedentes médicos de un paciente, resaltando en esta última que debemos aumentar la seguridad para mantener su integridad reconociendo las siguientes características de la información.

- ***Es crítica.*** Es indispensable para garantizar la continuidad operativa.

- Es *Valiosa*. Es un activo con valor en sí misma.
- Es *Sensitiva*. Debe ser conocida por las personas que la procesan y solo por ellas.

La integridad de la Información

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: La firma digital es uno de los pilares fundamentales de la seguridad de la información. (In SlideShare, 2015)

Disponibilidad de la Información

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran. En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlos, y

los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad de los sistemas objetivos, debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema. Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio. (CoreOne, 2015)

Privacidad de la Información

La protección de datos, también llamada privacidad de información, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros. (TechTarget, 2015)

Control de la Información

El control de la información es el proceso que garantiza que solo usuarios autorizados decidan cuando y como se puede tener acceso a la información.

Autenticidad de la Información

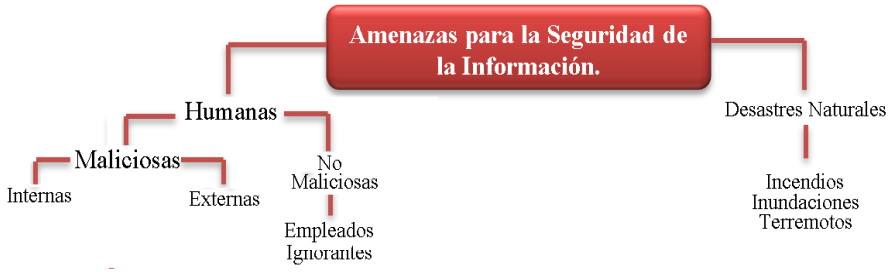
Permite identificar que la información solicitada es válida y puede ser utilizable en forma, tiempo y distribución. Mediante esta propiedad

podemos verificar el origen de la información a través de la validación del emisor de origen con la finalidad de evitar suplantaciones de identidades.

Las Amenazas

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información. Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales. (Departamento de Seguridad Informática, 2015)

Figura 2. Amenazas para la seguridad de la información



Realizado por: Los autores

Las amenazas pueden ser analizadas en tres situaciones o eventos; antes de que se efectúe el ataque, durante y después del mismo. Ante esto se deben conformar mecanismos y políticas que garanticen la integridad de nuestro sistema.

La Prevención (antes). Son mecanismos que garantizan la fiabilidad de un sistema para su normal funcionamiento, ejemplo el cifrado de la información para su posterior transmisión.

La Detección (durante). Son los mecanismos que están orientados a la detección de violaciones a la seguridad, generalmente software de auditoria.

La Recuperación (después). Son los mecanismos que intervienen cuando se ha detectado una filtración en el sistema, permitiendo el funcionamiento y ejecución normal de las actividades y tareas, por ejemplo, la recuperación desde copias de seguridad (backups).

Amenazas de personal interno

Las amenazas a la seguridad de un sistema, provenientes del personal del propio sistema informático, rara vez es tomada en cuenta porque se supone un ámbito de confianza muchas veces inexistente. Generalmente estos ataques son accidentes por desconocimiento o inexistencia de las normas básicas de seguridad; pero también pueden ser del tipo intencional.

Es de destacar que un simple electricista puede ser más dañino que el más peligroso de los piratas informáticos, ya que un corte de

energía puede causar un desastre en los datos del sistema. Al evaluar la situación, se verá que aquí el daño no es intencionado, pero ello no está en discusión; el daño existió y esto es lo que compete a la seguridad informática. (Segu Info, 2015)

Ex-empleados

Este grupo puede estar especialmente interesado en violar la seguridad de nuestra empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado para pasar a trabajar en la competencia. Generalmente se trata de personas descontentas con la organización que conocen a la perfección la estructura del sistema y tienen los conocimientos necesarios como para causar cualquier tipo de daño. También han existido casos donde el ex - empleado deja Bombas Lógicas que “explotan” tiempo después de marcharse. (Segu Info, 2015)

Intrusos remunerados

Por lo general son expertos informáticos que son contratados por terceros para que irrumpan en los sistemas informáticos y extraigan información confidencial, efectúen sabotajes informáticos, etc.

Fraudes, engaños y extorsiones

Los fraudes por internet son los que resultan cada vez más rentables pues estos son más difíciles prevenirlos, identificarlos y detenerlos. La información adecuada sobre las modalidades de fraude en internet puede disminuir las posibilidades de ser víctima de una estafa, aunque a veces estar informado no es suficiente también se necesita

la ayuda de un buen antivirus para lo que se recomienda comprar una licencia completa de antivirus. Un caso de Fraude, es el uso del Software Spyware, por parte de los atacantes, el cual recolecta y envía información privada sin el consentimiento y/o conocimiento del usuario; también se encuentra el Dialer, que realiza llamadas a través de módem o RDSI para conectar a internet utilizando números de tarificación adicional sin conocimiento del usuario; el Keylogger, el Adware, entre otros. Además, utilizan técnicas como la Ingeniería Social, el Phishing (roba la identidad del usuario por medio de correo electrónico), el Skimming (robo de información que contiene una tarjeta de Crédito), y otras más dependiendo del objetivo que tengan en mente. (Seguridad Informatica, 2015)

Por otro lado, se encuentran los engaños que generalmente suceden a través de correos electrónicos, ya que es una de las formas más habituales de difundir cadenas y muchas veces las personas no notan que dichas cadenas brindan información imprecisa la cual se pide circular, creando de esta manera posibilidades para que los atacantes afecten nuestro entorno. Un claro ejemplo de Engaño, se ve reflejado en los correos que contienen geoposicionamiento y supuestas frases para Facebook, el cual parece provenir de direcciones aleatorias, pero siempre desde personas que son contactos de quien recibe el correo, dejando claro que alguien inicialmente cae en la trampa y posteriormente, de forma automática se comienzan a enviar correos a los contactos. (Seguridad Informatica, 2015)

Finalmente, se considera el caso de Extorsión, consistente en la publicación o amenaza de publicación de alguna información difamatoria sobre la víctima, utilizando algún medio de la Red, luego, el chantaje a través de la Web se tiene en cuenta como un caso de Ciber-Extorsión, ya que, últimamente los atacantes acechan a cualquier persona que disponga de un sitio web, pidiendo dinero a cambio de divulgar información por internet acerca de éste, que pueda considerarse un agujero de seguridad, y que en muchas ocasiones el usuario no lo nota, y recurre a hacer evaluaciones de su sitio. (Seguridad Informatica, 2015)

Motivaciones de los atacantes

El FBI ha acuñado el acrónimo MICE para resumir las distintas motivaciones de los atacantes e intrusos en las redes de ordenadores: Money, Ideology, Compromise y Ego (Dinero, Ideología, Compromiso y Autorrealización Personal). (Alberto, 2009)

Consideraciones económicas

Simplemente realizan los ataques con el objetivo de efectuar operaciones fraudulentas, hurtar información confidencial que luego es vendida a terceros, realizar extorciones (es decir sino se cancela un determinado rescate se eliminará información o se dará de baja un sistema que haya sido comprometido), intentos de manipulación, etc.

Diversión

Un sin número de usuarios en internet efectúan estos ataques como

pasatiempo o simplemente como forma de pasar parte de su tiempo delatante del ordenador.

Ideología

Los atacantes tienen como objetivo de ataque a determinadas organizaciones, empresas y sitios webs gubernamentales, con un contenido claramente político.

Elementos a considerar en nuestra institución

En toda institución existen tres elementos fundamentales que debemos proteger:

- **El hardware**, componen el conjunto de los sistemas físicos (CPU, cableado de red, impresoras, cd-rom, memorias flash, componentes de comunicación, etc.)
- **El software**, componen aquellos elementos lógicos que hacen funcional al hardware (sistemas operativos, aplicaciones, utilitarios, etc.)
- **Los datos**, que representan al conjunto de información lógica que maneja el software (base de datos, documentos, archivos, etc.)

Los cuales pueden estar propensos a dos tipos de ataques que son:

Ataques Pasivos

Los ataques pasivos reciben su nombre debido a que el atacante (o perpetrador u oponente o persona que se entromete) no altera en ningún momento la información, es decir, únicamente la observa, escucha, obtiene o monitorea mientras está siendo transmitida. Cualquier

ataque pasivo tiene los siguientes objetivos principales: (Universidad Nacional Autonóma de México, 2015)

- **Intercepción de datos:** Consiste en el conocimiento de la información cuando existe una liberación de los contenidos del mensaje. (Universidad Nacional Autónoma de México, 2015)
- **Análisis de tráfico:** Consiste en la observación de todo tráfico que pasa por la red. (Universidad Nacional Autónoma de México, 2015)

Ataques Activos

Los ataques activos implican algún tipo de modificación del flujo de datos transmitido –modificación de la corriente de datos- o la creación de un falso flujo de datos –creación de una corriente falsa-. (Universidad Nacional Autónoma de México, 2015)

Los ataques activos pueden clasificarse de la siguiente manera:

- **Enmascaramiento o suplantación de identidad:** El intruso se hace pasar por una entidad diferente. (Universidad Nacional Autónoma de México, 2015)
- **Réplica o reactuación:** Uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado debido a que realiza una retransmisión subsecuente. (Universidad Nacional Autónoma de México, 2015)
- **Modificación de mensajes:** Una porción del mensaje legítimo es alterada, o los mismos mensajes son retardados o reordenados, esto provoca que se produzca un efecto no autorizado.

(Universidad Nacional Autónoma de México, 2015)

La seguridad Física de la Información

Es muy importante ser consciente que por más que nuestra empresa sea la más segura desde el punto de vista de ataques externos, Hackers, virus, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un incendio. La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma. Así, la Seguridad Física consiste 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 los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. (Segu Info, 2015)

Seguridad ante incendios

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas. El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas. Desgraciadamente los sistemas anti fuego dejan mucho que desear, causando casi igual

daño que el propio fuego, sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputos. (GITS Ciberseguridad, 2015)

Seguridad ante inundaciones

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputos. Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior. Para evitar este inconveniente se pueden tomar las siguientes medidas: Construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras. (GITS Ciberseguridad, 2015)

Seguridad ante condiciones climáticas

Normalmente se reciben por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares. Las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada. La frecuencia y severidad de su ocurrencia deben ser tenidas en cuenta al decidir la construcción de un edificio. La comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta

severa, permite que se tomen precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia. (GITS Ciberseguridad, 2015)

Seguridad ante terremotos

Estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. El problema es que, en la actualidad, estos fenómenos están ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros. (GITS Ciberseguridad, 2015)

Instalaciones eléctricas

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto, esta una de las principales áreas a considerar en la seguridad física. Además, es una problemática que abarca desde el usuario hogareño hasta la gran empresa. En la medida que los sistemas se vuelven más complicados se hace más necesaria la presencia de un especialista para evaluar riesgos particulares y aplicar soluciones que estén de acuerdo con una norma de seguridad industrial. (GITS Ciberseguridad, 2015)

La Ergometría

El enfoque ergonómico plantea la adaptación de los métodos, los objetos, las maquinarias, herramientas e instrumentos o medios y las condiciones de trabajo a la anatomía, la fisiología y la psicología

del operador. Entre los fines de su aplicación se encuentra, fundamentalmente, la protección de los trabajadores contra problemas tales como el agotamiento, las sobrecargas y el envejecimiento prematuro. (GITS Ciberseguridad, 2015)

La seguridad Lógica de la información

La evolución normal del concepto de seguridad en una sociedad de la información y el conocimiento, hace que las estrategias de seguridad de la antigüedad cobren vida en un mundo regido por los “ bits y bytes”.

Todas las condiciones de seguridad analizadas en el aparte anterior tienen sus equivalentes en el mundo de la informática y la tecnología. La Seguridad Lógica se refiere a que la información solo pueda ser accesible parcialmente según el puesto de la persona, de modo que solo el administrador del sistema y algún otro alto funcionario tenga acceso completo, eso previene fraudes y otros daños. Hay quienes incluyen en la seguridad lógica, la seguridad de la información, lo que incluye la protección contra virus, robos de datos, modificaciones, intrusiones no autorizadas, respaldos adecuados y demás cosas relacionadas. El activo más importante de un sistema informático es la información y, por tanto, la seguridad lógica se plantea como uno de los objetivos más importantes. Después de ver cómo nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información

por él almacenada y procesada. Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica. (GITS Ciberseguridad, 2015)

Controles de acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario. Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados. Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. (GITS Ciberseguridad, 2015)

Identificación y autenticación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso

y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación. Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas: (GITS Ciberseguridad, 2015)

- **Algo que solamente el individuo conoce:** Por ejemplo, una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc. (GITS Ciberseguridad, 2015)
- **Algo que la persona posee:** Por ejemplo, una tarjeta magnética. (GITS Ciberseguridad, 2015)
- **Algo que el individuo es y que lo identifica unívocamente:** Por ejemplo, las huellas digitales o la voz. (GITS Ciberseguridad, 2015)
- **Algo que el individuo es capaz de hacer:** Por ejemplo, los patrones de escritura. (GITS Ciberseguridad, 2015)

Los Roles

El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Algunos ejemplos de roles serían los siguientes: Programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc. En este caso los

derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios. (GITS Ciberseguridad, 2015)

Limitaciones a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario. (GITS Ciberseguridad, 2015)

Modalidades de acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser: (GITS Ciberseguridad, 2015)

- **Lectura:** El usuario puede únicamente leer o visualizar la información, pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa. (GITS Ciberseguridad, 2015)
- **Escritura:** Este tipo de acceso permite agregar datos, modificar o borrar información. (GITS Ciberseguridad, 2015)
- Ejecución: Este acceso otorga al usuario el privilegio de ejecutar programas. (GITS Ciberseguridad, 2015)
- **Borrado:** Permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es

considerado una forma de modificación. (GITS Ciberseguridad, 2015)

Control de acceso interno

Palabras Claves (passwords)

- Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo, cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica. Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: La elección de passwords débiles. Sería deseable usar passwords seguras ya que aquí radican entre el 90% y 99% de los problemas de seguridad planteados. (GITS Ciberseguridad, 2015)

Sincronización de Passwords

Consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios

hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que, si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad. (GITS Ciberseguridad, 2015)

Caducidad y control de Password

Este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen. (GITS Ciberseguridad, 2015)

Encriptación de la Información

Es el proceso mediante el cual cierta información o texto sin formato es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros. Opcionalmente puede existir además un proceso de desencriptación a través del cual la información puede ser interpretada de nuevo a su estado original, aunque existen métodos de encriptación que no pueden ser revertidos. (Encriptación de Datos, 2015)

Sistemas Biométricos

La biometría es una tecnología de identificación basada en el reconocimiento de una característica física e intransferible de las personas, como, por ejemplo, la huella digital, el reconocimiento del patrón venoso del dedo o el reconocimiento facial. La biometría es un excelente sistema de identificación de la persona que se aplica en muchos procesos debido a dos razones fundamentales, la seguridad y la comodidad. Entre las aplicaciones de identificación con biometría están el control de acceso biométrico, el control de presencia biométrico, el logon biométrico para aplicaciones de software a sistemas operativos o cualquier otra aplicación de identificación mediante la incorporación de un lector biométrico para integración. (Kimaldi, 2015)

Dispositivos de control de puertos

Estos dispositivos autorizan el acceso a un determinado puerto que puede estar físicamente separado o incluido en otro dispositivo de comunicación, por ejemplo, los módems. (GITS Ciberseguridad, 2015)

Firewalls o cortafuegos

En la actualidad, un firewall es una herramienta indispensable para proteger nuestra conexión a Internet. El hecho de hacer uso de una conexión a Internet puede ser causa de múltiples ataques a nuestro equipo de cómputo desde el exterior, cuanto más tiempo estemos en línea, mayor es la probabilidad de que la seguridad de nuestro sistema

se vea comprometida por un intruso desconocido, Por lo tanto, ya no solamente es necesario tener instalado y actualizado un software antivirus y un software antispyware sino también es totalmente recomendable mantener instalado y actualizado un software de firewall. Un firewall es un sistema diseñado para impedir el acceso no autorizado o el acceso desde una red privada. Pueden implementarse firewalls en hardware, software o en ambos. Los firewalls se utilizan con frecuencia para impedir que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet. El firewall personal protege al equipo frente a ataques de Internet, contenidos Web peligrosos, análisis de puertos y otros comportamientos de naturaleza sospechosa. (Jesús & Rocío del Pilar, 2015)

LAS VULNERABILIDADES

Capítulo 2

LAS VULNERABILIDADES

Las vulnerabilidades son el resultado de bugs o de fallos en el diseño del sistema. Aunque, en un sentido más amplio, también pueden ser el resultado de las propias limitaciones tecnológicas, porque, en principio, no existe sistema 100% seguro. Por lo tanto, existen vulnerabilidades teóricas y vulnerabilidades reales (conocidas como exploits). Las vulnerabilidades en las aplicaciones suelen corregirse con parches, hotfixs o con cambios de versión. En tanto algunas otras requieren un cambio físico en un sistema informático. Las vulnerabilidades se descubren muy seguido en grandes sistemas, y el hecho de que se publiquen rápidamente por todo internet (mucho antes de que exista una solución al problema), es motivo de debate. Mientras más conocida se haga una vulnerabilidad, más probabilidades de que existan piratas informáticos que quieren aprovecharse de ellas. (ALEGSA.com.ar, 2015)

Las vulnerabilidades en los sistemas de información

Las vulnerabilidades son debilidades internas de un Sistema de Información las cuales, si son explotadas, podrían causar un daño significativo. La existencia de una vulnerabilidad no causa por sí misma un daño, es necesario que se presente una amenaza para detonarla. De esta manera, la vulnerabilidad es una deficiencia en el diseño, implementación, operación o los controles internos en un proceso, que podría utilizarse para violar la seguridad de un sistema. Ahora bien, una vulnerabilidad que no tiene su correspondiente

amenaza, puede que no requiera la implantación de un control, pero aun así debe ser reconocida y monitoreada para cambiarla. Todos los Sistemas de Información tienen vulnerabilidades. Debemos considerar que éstos son desarrollados, implementados y operados por personas, por lo tanto, el error está presente intrínsecamente en todos ellos. Sin duda, existen casos en los cuales el administrador o programador instalan maliciosamente una falla en un sistema para ser detonados posteriormente. Asimismo, la mayoría de las vulnerabilidades surgen de factores tales como la complejidad, la ignorancia o el costo de los controles financieros. El punto para la gestión de riesgos y las auditorías es la identificación y corrección de las vulnerabilidades antes de que puedan ser utilizadas, o por lo menos, para limitar el rango de aplicación de las amenazas que puedan valerse de ellas, hasta el punto de que ya no sean creíbles. (Cas-Chile, 2015)

Identificación de las amenazas

La identificación de amenazas nos permite reconocer los posibles ataques a lo que están propensos los sistemas, identificando la forma como opera el atacante, sus objetivos y los tipos de acceso que utiliza para cumplir con su objetivo. Un ataque dirigido hacia nuestra institución o empresa nos podría dejar consecuencias que se describen a continuación.

- **Data Corruption.** La información es alterada y pasa a ser obsoleta.
- **Denial of Services (DoS).** Los servicios de los sistemas que

deberían estar disponibles no lo están.

- **Leakage.** Los paquetes de datos llegan a terceras personas.

Desde el año 1990 hasta la actualidad, el CERT ha desarrollado estudios estadísticos que demuestran que cada vez son más frecuentes los ataques tipo informático y a su vez más sofisticados y difíciles de monitorear.

Sistema de detección de intrusos IDS

Un sistema de detección de intrusos es un componente más dentro del modelo de seguridad de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómalas desde el exterior-interior de un sistema informático. Los sistemas de detección de intrusos pueden clasificarse, según su función y comportamiento en: (Segu Info, 2015)

- **Host-Based IDS:** Operan en un host para detectar actividad maliciosa en el mismo. (Segu Info, 2015)
- **Network-Based IDS:** Operan sobre los flujos de información intercambiados en una red. (Segu Info, 2015)
- **Knowledge-Based IDS:** Sistemas basados en Conocimiento. (Segu Info, 2015)
- **Behavior-Based IDS:** Sistemas basados en Comportamiento. Se asume que una intrusión puede ser detectada observando una desviación respecto del comportamiento normal o esperado de un usuario en el sistema. (Segu Info, 2015)

La idea central de este tipo de detección es el hecho de que la actividad intrusiva es un conjunto de actividades anómalas. Si alguien consigue entrar de forma ilegal al sistema, no actuará como un usuario comprometido; su comportamiento se alejará del de un usuario normal. Sin embargo, en la mayoría de las ocasiones una actividad intrusiva resulta del agregado de otras actividades individuales que por sí solas no constituyen un comportamiento intrusivo de ningún tipo. Así las intrusiones pueden clasificarse en: (Segu Info, 2015)

- **Intrusivas, pero no anómalas:** Denominados Falsos Negativos (el sistema erróneamente indica ausencia de intrusión). En este caso la actividad es intrusiva pero como no es anómala no es detectada. No son deseables, porque dan una falsa sensación de seguridad del sistema. (Segu Info, 2015)
- **No intrusivas pero anómalas:** Denominados Falsos Positivos (el sistema erróneamente indica la existencia de intrusión). En este caso la actividad es no intrusiva, pero como es anómala el sistema "decide" que es intrusiva. Deben intentar minimizarse, ya que en caso contrario se ignorarán los avisos del sistema, incluso cuando sean acertados. (Segu Info, 2015)
- **No intrusiva ni anómala:** Son Negativos Verdaderos, la actividad es no intrusiva y se indica como tal. (Segu Info, 2015)
- **Intrusiva y anómala:** Se denominan Positivos Verdaderos, la actividad es intrusiva y es detectada. (Segu Info, 2015)

Los detectores de intrusiones anómalas requieren mucho gasto computacional, ya que se siguen normalmente varias métricas para determinar cuánto se aleja el usuario de lo que se considera comportamiento normal. (Segu Info, 2015)

Características de los IDS

Cualquier sistema de detección de intrusos debería, sea cual sea el mecanismo en que esté basado, debería contar con las siguientes características: (Segu Info, 2015)

- Debe funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en background dentro del equipo que está siendo observado. Sin embargo, no debe ser una "caja negra" (debe ser examinable desde el exterior). (Segu Info, 2015)
- Debe ser tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema. (Segu Info, 2015)

En relación con el punto anterior, debe ser resistente a perturbaciones. El sistema puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado. (Segu Info, 2015)

- Debe imponer mínima sobrecarga sobre el sistema. Un sistema que relentiza la máquina, simplemente no será utilizado. (Segu Info, 2015)
- Debe observar desviaciones sobre el comportamiento estándar. (Segu Info, 2015)
- Debe ser fácilmente adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones. (Segu Info, 2015)
- Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo. (Segu Info, 2015)
- Debe ser difícil de "engañar". (Segu Info, 2015)

Fortalezas de los IDS

- Suministra información muy interesante sobre el tráfico malicioso de la red. (Segu Info, 2015)
- Poder de reacción para prevenir el daño. (Segu Info, 2015)
- Es una herramienta útil como arma de seguridad de la red. (Segu Info, 2015)
- Ayuda a identificar de dónde provienen los ataques que se sufren. (Segu Info, 2015)
- Recoge evidencias que pueden ser usadas para identificar intrusos. (Segu Info, 2015)
- Es una "cámara" de seguridad y una "alarma" contra ladrones. (Segu Info, 2015)
- Funciona como "disuasor de intrusos". (Segu Info, 2015)
- Alerta al personal de seguridad de que alguien está tratando de entrar. (Segu Info, 2015)
- Protege contra la invasión de la red. (Segu Info, 2015)
- Suministra cierta tranquilidad. (Segu Info, 2015)
- Es una parte de la infraestructura para la estrategia global de

defensa. (Segu Info, 2015)

- La posibilidad de detectar intrusiones desconocidas e imprevistas. Pueden incluso contribuir (parcialmente) al descubrimiento automático de esos nuevos ataques. (Segu Info, 2015)
- Son menos dependientes de los mecanismos específicos de cada sistema operativo. (Segu Info, 2015)
- Pueden ayudar a detectar ataques del tipo "abuso de privilegios" que no implica realmente ninguna vulnerabilidad de seguridad. En pocas palabras, se trata de una aproximación a la paranoia: "Todo aquello que no se ha visto previamente es peligroso". (Segu Info, 2015)
- Menor costo de implementación y mantenimiento al ubicarse en puntos estratégicos de la red. (Segu Info, 2015)

Tipos de IDS

Entender que es un IDS y las funciones que proporciona, es clave para determinar cuál será el tipo apropiado para incluir en una política de seguridad de computación. Esta sección discute los conceptos detrás de los IDSes, las funcionalidades de cada tipo de IDS y la aparición de los IDSes híbridos, que emplean varias técnicas de detección y herramientas en un solo paquete. Algunos IDSes están basados en conocimiento, lo que alerta a los administradores de seguridad antes de que ocurra una intrusión usando una base de datos de ataques comunes. Alternativamente, existen los IDS basados en comportamiento, que hacen un seguimiento de todos los recursos usados buscando cualquier

anomalía, lo que es usualmente una señal positiva de actividad maliciosa. Algunos IDSes son servicios independientes que trabajan en el fondo y escuchan pasivamente la actividad, registrando cualquier paquete externo sospechoso. Otros combinan las herramientas de sistemas estándar, configuraciones modificadas y el registro detallado, con la intuición y la experiencia del administrador para crear un kit poderoso de detección de intrusos. Evaluando las diferentes técnicas de detección de intrusos lo ayudará a encontrar aquella que es adecuada para su organización. Los tipos más importantes de IDSes mencionados en el campo de seguridad son conocidos como IDSes basados en host y basados en red. Un IDSes basado en host es el más completo de los dos, que implica la implementación de un sistema de detección en cada host individual. Sin importar en qué ambiente de red resida el host, estará protegido. Un IDS basado en la red filtra los paquetes a través de un dispositivo simple antes de comenzar a enviar a host específicos. Los IDSes basados en red a menudo se consideran como menos completos puestos que muchos hosts en un ambiente móvil lo hacen indisponible para el escaneo y protección de paquetes de red. (Red Hat Enterprise Linux 4: Manual de seguridad, 2015)

IDS basados en host

Un IDS basado en host analiza diferentes áreas para determinar el uso incorrecto (actividades maliciosas o abusivas dentro de la red) o alguna intrusión (violaciones desde afuera). Los IDS basados en host consultan diferentes tipos de registros de archivos (kernel, sistema, servidores,

red, cortafuegos, y más) y comparan los registros contra una base de datos interna de peculiaridades comunes sobre ataques conocidos. Los IDS basados en host de Linux y Unix hacen uso extensivo de syslog y de su habilidad para separar los eventos registrados por severidad (por ejemplo, mensajes menores de impresión versus advertencias importantes del kernel). El comando syslog está disponible cuando se instala el paquete sysklogd, incluido con Red Hat Enterprise Linux. Este paquete proporciona el registro de mensajes del sistema y del kernel. Los IDS basados en hosts filtran los registros (lo cual, en el caso de algunas redes y registros de eventos del kernel pueden ser bastante detallados), los analizan, vuelven a etiquetar los mensajes anómalos con su propia clasificación de severidad y los reúne en su propio registro para que sean analizados por el administrador. Los IDS basados en host también pueden verificar la integridad de los datos de archivos y ejecutables importantes. Funciona verificando una base de datos de archivos confidenciales (y cualquier archivo añadido por el administrador) y crea una suma de verificación de cada archivo con una utilidad de resumen de archivos de mensajes tal como md5sum (algoritmo de 128-bit) o sha1sum (algoritmo de 160-bit). El IDS basado en host luego almacena las sumas en un archivo de texto plano y periódicamente compara las sumas de verificación contra los valores en el archivo de texto. Si cualesquiera de estas sumas no coinciden, el IDS alertará al administrador a través de un correo electrónico o a un mensaje al celular. (Red Hat Enterprise Linux 4: Manual de seguridad,

2015)

IDS basados en la red

Los sistemas de detección de intrusos basados en la red operan de una forma diferente que aquellos IDS basados en host. La filosofía de diseño de un IDS basado en la red es escanear los paquetes de red al nivel del enrutador o host, auditar la información de los paquetes y registrar cualquier paquete sospechoso en un archivo de registros especial con información extendida. Basándose en estos paquetes sospechosos, un IDS basado en la red puede escanear su propia base de datos de firmas de ataques a la red y asignarles un nivel de severidad para cada paquete. Si los niveles de severidad son lo suficientemente altos, se enviará un correo electrónico o un mensaje de página de advertencia a los miembros del equipo de seguridad para que ellos puedan investigar la naturaleza de la anomalía. Los IDS basados en la red se han vuelto muy populares a medida en que la Internet ha crecido en tamaño y tráfico. Los IDS que son capaces de escanear grandes volúmenes de actividad en la red y exitosamente etiquetar transmisiones sospechosas, son bien recibidos dentro de la industria de seguridad. Debido a la inseguridad inherente de los protocolos TCP/IP, se ha vuelto imperativo desarrollar escáner, husmeadores y otras herramientas de auditoría y detección para así prevenir violaciones de seguridad por actividades maliciosas en la red, tales como: (Red Hat Enterprise Linux 4: Manual de seguridad, 2015)

- Engaño de direcciones IP (IP Spoofing)
- Ataques de rechazo de servicio (DoS)
- Envenenamiento de caché arp
- Corrupción de nombres DNS
- Ataques de hombre en el medio

TIPOS DE ATAQUES INFORMÁTICOS

Capítulo 3

TIPOS DE ATAQUES INFORMÁTICOS.

Ingeniería Social

Como término se refiere o define un conjunto de técnicas psicológicas y también habilidades sociales que se utilizan de forma consciente para lograr la obtención de información de terceras personas o para lograr que una o persona realice las acciones que permita al ingeniero social lograr su objetivo. Todo esto atacando y aprovechando los errores y/o vulnerabilidades humanas. En la informática, así como existen personas expertas en realizar delitos, hackear y crackear sistemas vulnerando los softwares informáticos, también existen personas que son expertas en engañar y manipular a otras personas para poder lograr objetivos como conseguir datos para acceder a algún sistema o cuentas personales ya sean de redes sociales o bancarias, y en sí a cualquier información que sea de carácter privado. (Sebastián & Nelson, 2015)

Ingeniería Social Inversa

La ingeniería social inversa describe una situación en la que el atacante crea una persona que parece estar en una posición de autoridad y al cual, a diferencia de otros ataques, los empleados se dirigirán para solicitarle información. Es una técnica muy poderosa pero muy difícil de llevar a cabo pues exige una gran cantidad de recursos y tiempo en la investigación y preparación del ataque. A diferencia de la ingeniería social donde el individuo se muestra más activo, poniéndose en contacto con las personas que pueden suministrarle la información necesaria para atacar o introducirse en un sistema, la ingeniería social inversa es

pasiva, ya que en ella se pone la trampa y se espera cautelosamente a que alguien caiga en ella (la trampa puede estar dirigida a un colectivo concreto o bien a una generalidad de usuarios). (Sebastián & Nelson, 2015)

Phishing

El termino Phishing es utilizado para referirse a uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima. El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas. (InfoSpyware, 2015)

Ataques de suplantación de Identidad.

Spoofing

Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque -al menos la idea- es muy sencilla: Desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado. Y como los anillos de confianza

basados en estas características tan fácilmente falsificables son aún demasiado abundantes (no tenemos más que pensar en los comandos r-, los accesos NFS, o la protección de servicios de red mediante TCP Wrapper), el spoofing sigue siendo en la actualidad un ataque no trivial, pero factible contra cualquier tipo de organización. (Zona Virus, 2015)

IP Spoofing

Suplantación o falseamiento de IP, hacer creer que somos quien no somos. No confundir spoofear una IP con anonimizar una IP. El spoofing trae consigo el anonimato, pero sería como un anonimato "a elegir", esto es, apropiarse de la IP de otro usuario de la red.

Consiste en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar. Esto se consigue generalmente gracias a programas destinados a ello y puede ser usado para cualquier protocolo dentro de TCP/IP como ICMP, UDP o TCP. Hay que tener en cuenta que las respuestas del host que reciba los paquetes irán dirigidas a la IP falsificada. Por ejemplo, si enviamos un ping (paquete ICMP "echo request") spoofeado, la respuesta será recibida por el host al que pertenece la IP legalmente. Este tipo de spoofing unido al uso de peticiones broadcast a diferentes redes es usado en un tipo de ataque de flood conocido como smurf ataque. Para poder realizar IP SPOOFING en sesiones TCP, se debe tener en cuenta el comportamiento de dicho protocolo con el envío de paquetes SYN y ACK con su ISN específico y teniendo en cuenta que el propietario real de la IP podría (si no se le impide de alguna manera) cortar la

conexión en cualquier momento al recibir paquetes sin haberlos solicitado. También hay que tener en cuenta que los routers actuales no admiten el envío de paquetes con IP origen no perteneciente a una de las redes que administra (los paquetes spoofeados no sobrepasarán el router). (Hacking Etico, 2015)

DNS Spoofing

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Su principal función es la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. Por ejemplo, al acceder a www.google.com, si nuestro navegador no conoce su dirección IP realizará una consulta al servidor DNS para que este le diga cuál es la IP que le corresponde y así accederá a la página mediante su IP y mostrará su contenido. Pharming es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domain name) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio. El DNS Spoofing hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre, es decir, resolver con una dirección IP falsa un cierto nombre DNS o viceversa.

Esto se puede conseguir de diferentes formas, desde modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones dirección-nombre, hasta comprometiendo un servidor que infecte la caché de otro (lo que se conoce como DNS Poisoning); incluso sin acceso a un servidor DNS real, un atacante puede enviar datos falseados como respuesta a una petición de su víctima sin más que averiguar los números de secuencia correctos. (Hacking Etico, 2015)

Web Spoofing

Suplantación de una página web real. Enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información de dicha víctima (páginas WEB vistas, información de formularios, contraseñas etc.). El atacante puede monitorear todas las actividades que realiza la víctima. La página WEB falsa actúa a modo de proxy solicitando la información requerida por la víctima a cada servidor original y saltándose incluso la protección SSL. La víctima puede abrir la página web falsa mediante cualquier tipo de engaño, incluso abriendo un simple LINK. Las personas que usan internet a menudo toman decisiones relevantes basadas en las señales del contexto que perciben. Por ejemplo, se podría decidir teclear los datos bancarios porque se cree que se está visitando el sitio del banco. Esta creencia se podría producir porque la página tiene un parecido importante, sale su URL en la barra de navegación, y por alguna que otra razón más. (Hacking Ético, 2015)

Captura de cuentas de usuarios y contraseñas.

Existen métodos que permiten suplantar la identidad de los usuarios gracias a herramientas como software espías o dispositivos hardware especializado en capturar las pulsaciones en el teclado de un computador comúnmente conocido como keyloggers, además es posible acceder a soluciones disponibles en el mercado web como KeyGhost o key Logger.

Snooping

El snooping DHCP es una función que determina cuáles son los puertos de switch que pueden responder a solicitudes de DHCP. Los puertos se identifican como confiables o no confiables. Los puertos confiables pueden recibir todos los mensajes de DHCP, los no confiables sólo pueden recibir solicitudes. Los puertos confiables de los hosts se alojan en el servidor de DHCP o pueden ser un enlace hacia dicho servidor. Si un dispositivo malicioso de un puerto no confiable intenta enviar un paquete de respuesta de DHCP a la red, el puerto se desactiva. Esta función puede unirse con las opciones de DHCP donde la información del switch, como el ID de puerto o la solicitud de DHCP pueden insertarse en el paquete de solicitudes de DHCP. (Ataques en redes LAN, 2015)

Ataques de tipo Cross-Site Scripting (XSS)

El XSS se trata de una vulnerabilidad que muchos desarrolladores web dejan pasar, bien por falta de planificación o por desconocimiento. Esta vulnerabilidad suele aparecer por la falta de mecanismos en el

filtrado de los campos de entrada que dispone la web, permitiendo el envío de datos e incluso la ejecución de scripts completos. El código malicioso utilizado en este tipo de ataques está compuesto por cadena de datos: Scripts completos contenidos en enlaces o ejecutados desde formularios vulnerables. (HOSTALIA.com, 2015)

Ataques de inyección de código SQL

La inyección de código SQL es un ataque en el cual se inserta código malicioso en las cadenas que posteriormente se pasan a una instancia de SQL Server para su análisis y ejecución. Todos los procedimientos que generan instrucciones SQL deben revisarse en busca de vulnerabilidades de inyección de código, ya que SQL Server ejecutará todas las consultas recibidas que sean válidas desde el punto de vista sintáctico. Un atacante cualificado y con determinación puede manipular incluso los datos con parámetros. La forma principal de inyección de código SQL consiste en la inserción directa de código en variables especificadas por el usuario que se concatenan con comandos SQL y se ejecutan. Existe un ataque menos directo que inyecta código dañino en cadenas que están destinadas a almacenarse en una tabla o como metadatos. Cuando las cadenas almacenadas se concatenan posteriormente en un comando SQL dinámico, se ejecuta el código dañino. El proceso de inyección consiste en finalizar prematuramente una cadena de texto y anexar un nuevo comando. Como el comando insertado puede contener cadenas adicionales que se hayan anexado al mismo antes de su ejecución, el atacante pone fin a la cadena inyectada

con una marca de comentario "--". El texto situado a continuación se omite en tiempo de ejecución. (TechNet, 2015)

Ataques de Monitorización

Los ataques de monitorización consisten en la observación y análisis de la víctima y su sistema, con el propósito de obtener información, identificar las vulnerabilidades de su sistema y establecer posibles formas de acceso en un futuro.

Shoulder Surfing

Consiste en espiar físicamente a los usuarios para obtener el login y su password correspondiente. El Surfing explota el error de los usuarios de dejar su login y password anotadas cerca de la computadora (generalmente en post–it adheridos al monitor o teclado). Cualquier intruso puede pasar por ahí, verlos y memorizarlos para su posterior uso. Otra técnica relacionada al surfing es aquella mediante la cual se ve, por encima del hombro, al usuario cuando teclea su nombre y password. (Segu Info, 2015)

Decoy (Señuelos)

Los Decoy son programas diseñados con la misma interface que otro original. En ellos se imita la solicitud de un logeo y el usuario desprevenido lo hace. Luego, el programa guardará esta información y dejará paso a las actividades normales del sistema. La información recopilada será utilizada por el atacante para futuras "visitas". Una técnica semejante es aquella que, mediante un programa se guardan todas las teclas presionadas durante una sesión. Luego solo hará falta

estudiar el archivo generado para conocer nombres de usuarios y claves. (Segu Info, 2015)

Scanning (Búsqueda)

El Scaneo, como método de descubrir canales de comunicación susceptibles de ser explotados, lleva en uso mucho tiempo. La idea es recorrer (scanear) tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular. Muchas utilidades de auditoría también se basan en este paradigma. El Scaneo de puertos pertenece a la Seguridad Informática desde que era utilizado en los sistemas de telefonía. Dado que actualmente existen millones de números de teléfono a los que se pueden acceder con una simple llamada, la solución lógica (para encontrar números que puedan interesar) es intentar conectarlos a todos. (Segu Info, 2015)

Ataques de Autenticación.

Reciben su nombre de una técnica utilizada por los atacantes o hackers de equipos personales (PC) para dominar el equipo atacado. Este tipo de ataque tiene como objetivo engañar al sistema de la víctima para ingresar al mismo. Generalmente este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y password. (EcuRed, 2015)

Backdoors

Los backdoors son utilizados para acceder a los sistemas, espiar o realizar actividades maliciosas en ellos. La diferencia entre este tipo

de virus y un troyano puede no estar tan clara. El backdoor es un tipo de troyano, que permite el acceso al sistema infectado y su control remoto. El atacante puede eliminar y modificar archivos, ejecutar programas, enviar correos de forma masiva o instalar herramientas maliciosas. Esto nos indica que los backdoors y los troyanos no son la misma cosa, aunque también es importante mencionar que hoy en día, los troyanos incorporan algunas funcionalidades del backdoor para poder acceder a la máquina infectada cuando se desee y seguir realizando las actividades maliciosas. Sin embargo, un backdoor puro puede venir previamente instalado en el sistema o en aplicaciones ya utilizadas por el usuario, ya sea porque el desarrollador olvidó quitar o bloquear esa función o porque lo dejó así a propósito. Es como una entrada secreta a una fortaleza, oculta para la mayoría y que pocos conocen, quienes lo hacen pueden aprovecharla sin ser vistos. (Phonet & Comunicaciones, 2015)

Exploits

Un Exploit es un programa o código que "explota" una vulnerabilidad del sistema o de parte de él para aprovechar esta deficiencia en beneficio del creador del mismo. Si bien el código que explota la vulnerabilidad no es un código malicioso en sí mismo, generalmente se lo utiliza para otros fines como permitir el acceso a un sistema o como parte de otros malware como gusanos y troyanos. Es decir que actualmente, los exploits son utilizados como "componente" de otro malware ya que al explotar vulnerabilidades del sistema permite hacer uso de funciones

que no estarían permitidas en caso normal. Existen diversos tipos de exploits dependiendo las vulnerabilidades utilizadas y son publicados cientos de ellos por día para cualquier sistema y programa existente pero sólo una gran minoría son utilizados como parte de otros malware (aquellos que pueden ser explotados en forma relativamente sencilla y que pueden lograr gran repercusión). (Segu Info, 2015)

CASO DE USO DE UN ATAQUE INFORMÁTICO

Capítulo 4

CASO DE USO DE UN ATAQUE INFORMÁTICO

Paso 1: Identificación de aquello que hay que proteger

El primer paso para el análisis de riesgos es la identificación de los elementos de valor que pueden verse en peligro en caso de un ataque. A estos elementos de valor los denominaremos activos y serán representados en forma de bolsa con la simbología de $ (dólar).

Es probable que los responsables del departamento de sistemas admitan que los principales activos que pueden ser afectados por un ataque informático y que deberían ser resguardados sería:

- La información estratégica y administrativa de la institución.
- Las bases de datos que contienen contraseñas y datos identificativos.
- Usuarios y contraseñas de accesos a los sistemas de información.
- La reputación de la institución y la ventaja competitiva de la compañía.

Figura 3. Identificación de aquello que hay que proteger

Realizado por: Los autores

Paso 2: Sucesos que tememos que puedan ocurrir

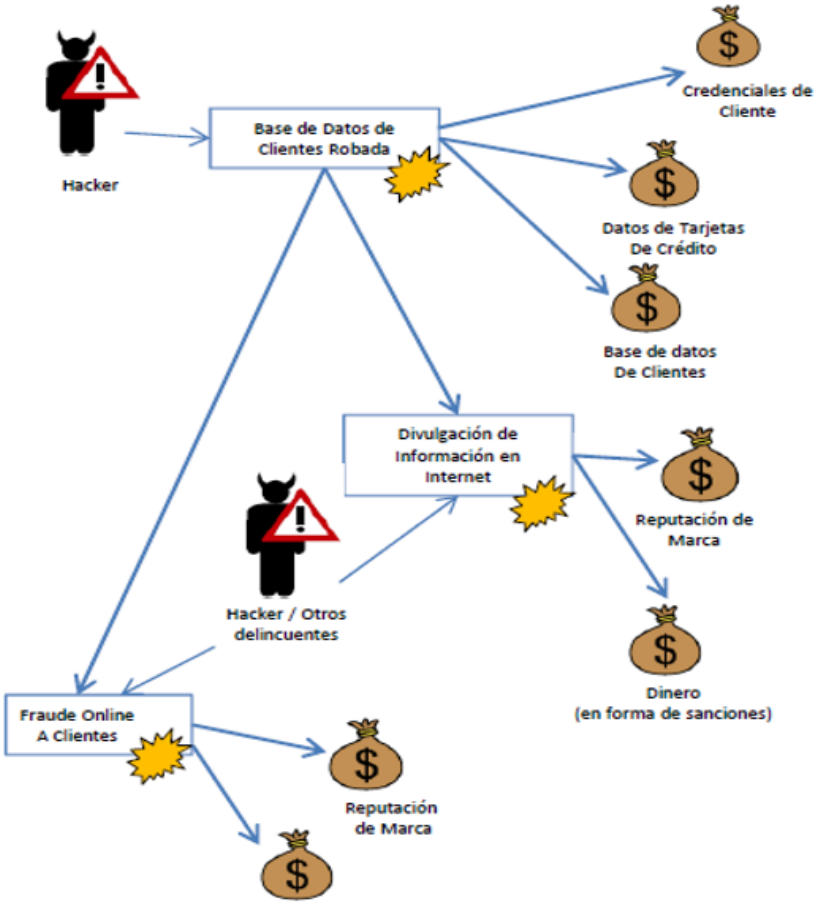
Luego de haber identificado los activos de valor para la institución el siguiente paso es evaluar qué consecuencias podrían derivarse a causa de una intrusión de amenaza en los sistemas de información de la institución. Para nuestro caso de estudio identificaremos los siguientes:

- El hurto de bases de datos de los usuarios.
- La circulación de los datos de las personas y usuarios en la web.
- El uso de los datos de las víctimas para realizar acciones ilícitas.
- Venta de información confidencial de la institución a la competencia.
- Hurto de información gestionada por la institución para efectuar inversiones, presupuestos de proyectos, planificaciones, pagos, etc.

En los siguientes diagramas se plasmarán dichos incidentes antes detallados, como también se identificarán a quienes lo efectúan (hackers, competencia, personas mal intencionadas, etc.) además identificaremos los activos de la institución que serían afectados.

En el diagrama plasmado a continuación se denotan los efectos ocasionados por el hurto de información de los clientes/usuarios y la práctica de actos perjudiciales contra los mismos, además observaremos como tales acciones podrían afectar la reputación de la marca de la institución, el daño causado a los clientes/usuarios y los cargos que la institución tendría que asumir.

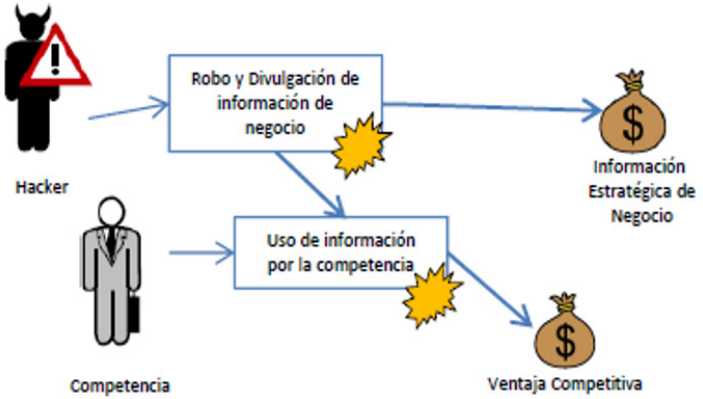
Figura 4. Efectos ocasionados por el hurto de información



Realizado por: Los autores

En el presente diagrama de caso de uso representaremos el hurto de información confidencial de la institución y la venta de dichos datos a la competencia.

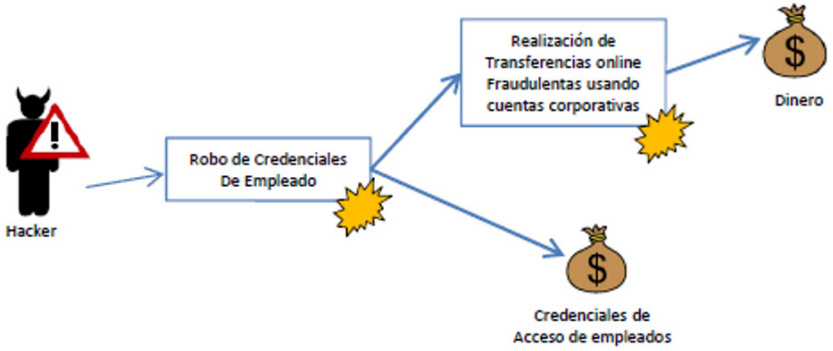
Figura 5. Hurto de información confidencial



Realizado por: Los autores

En el siguiente diagrama se simboliza el hurto de claves usadas por el departamento de recursos humanos y su posterior uso por los hackers para efectuar operaciones ilícitas.

Figura 6. Hurto de claves de acceso



Realizado por: Los autores

Paso 3: Entender cómo pueden llegar a producirse los sucesos

Para evitar que se produzcan sucesos no deseados identificados en los pasos anteriores, sería de gran ayuda constar con expertos especializados en seguridad informática, además de la capacitación del personal de la institución acerca del tema de seguridad y protección de la información para que obtengan conocimientos con la finalidad de evitar cualquier tipo de ataque informático dirigido a la institución.

Generalmente las etapas habituales para ejecutar un ataque informático son:

Estudio preliminar de la víctima y preparación de estrategias.

Mediante el uso de información pública de la institución los atacantes pueden identificar empleados víctimas para poder ejecutar un ataque inicial, asimismo les ayudará a definir tácticas de ataque.

Ataque inicial e infiltración

Para nuestro caso de estudio haremos la suposición que los atacantes harán uso de software espía dirigido a los ordenadores de las víctimas para poder aprovechar alguna vulnerabilidad de las aplicaciones instaladas como por ejemplo navegadores de internet o lectores de archivos (pdf, rar, etc.). Además, admitiremos que los atacantes incluirán enlaces en el software espía, que redireccionarán a mails fraudulentos para que los empleados víctimas accedan a los mismos.

Para que el ataque inicial tenga gran probabilidad de éxito debe suscitarse el siguiente escenario.

- Los mails deben ser creíbles para las víctimas. Para tal objetivo los atacantes harán uso de toda información relevante de la institución como también de los empleados.
- La instalación del software espía debe facilitarse mediante la explotación de vulnerabilidades de aplicaciones habituales que no hayan sido aún publicadas.
- La(s) víctima(s) deberá(n) tener acceso a la web desde su estación de trabajo además deberá acceder al enlace espía sin ningún tipo de desconfianza para que se pueda ejecutar el software camuflado.

Si esta etapa de ataque tiene éxito, como resultado vamos a obtener que el ordenador de la víctima quedará infectado y permitirá que el software espía establezca contacto con el centro de control del atacante.

Establecimiento de un punto de apoyo

Una vez establecido contacto con el centro de control del intruso, estos procederán a descargar software adicional en el ordenador de la víctima para poder facilitar y ocultar actividades posteriores. El modo de comunicación del software espía con el centro de control del intruso podrá ser ejecutado mediante el uso de comandos o la utilización de consolas remotas interactivas.

Pero, sin embargo, el éxito de la intrusión dependerá de que la actividad de control que establezca el intruso sea totalmente sigilosa y que esta disimulada al máximo en el tráfico legítimo de navegación por la web de la víctima. Independientemente del método de ataque empleado para vulnerar la seguridad de los sistemas, en esta fase los atacantes habrán conseguido establecer puntos de apoyo para poder ejecutar

sus actividades obteniendo además que el software espía tenga una funcionabilidad completa de hackeo y sea capaz de enviar mediante la web reportes de actividades ejecutadas por las víctimas.

Consolidación de la intrusión, ocultando la presencia

Las actividades siguientes a ejecutarse en el ordenador de la víctima estarán orientadas en la realización de modificaciones para ocultar al máximo los movimientos de los intrusos y pasar por desapercibidos. Para tal objetivo, los atacantes analizarán toda la información necesaria disponible para lograr ser usuarios administradores del ordenador de la víctima.

Exploración y movimiento

A partir de este punto, los intrusos iniciarán actividades de exploración de la red de la institución con el fin de localizar servidores y ordenadores que almacenen información de gran interés. Los intrusos mediante el uso de software y técnicas de hacking tratarán de comprometer contraseñas de administradores y accesos a bases de datos especialmente de administradores de grupos de dominio ya que estos proporcionarán llaves de acceso a otros ordenadores con el propósito de infectarlos con software espía y lograr tener el control total sobre los mismos. Con tal acceso obtenido y expandidos en la red de la institución los atacantes tendrán acceso a información, documentos, correos electrónicos, bases de datos y toda información digital que represente dinero para el atacante.

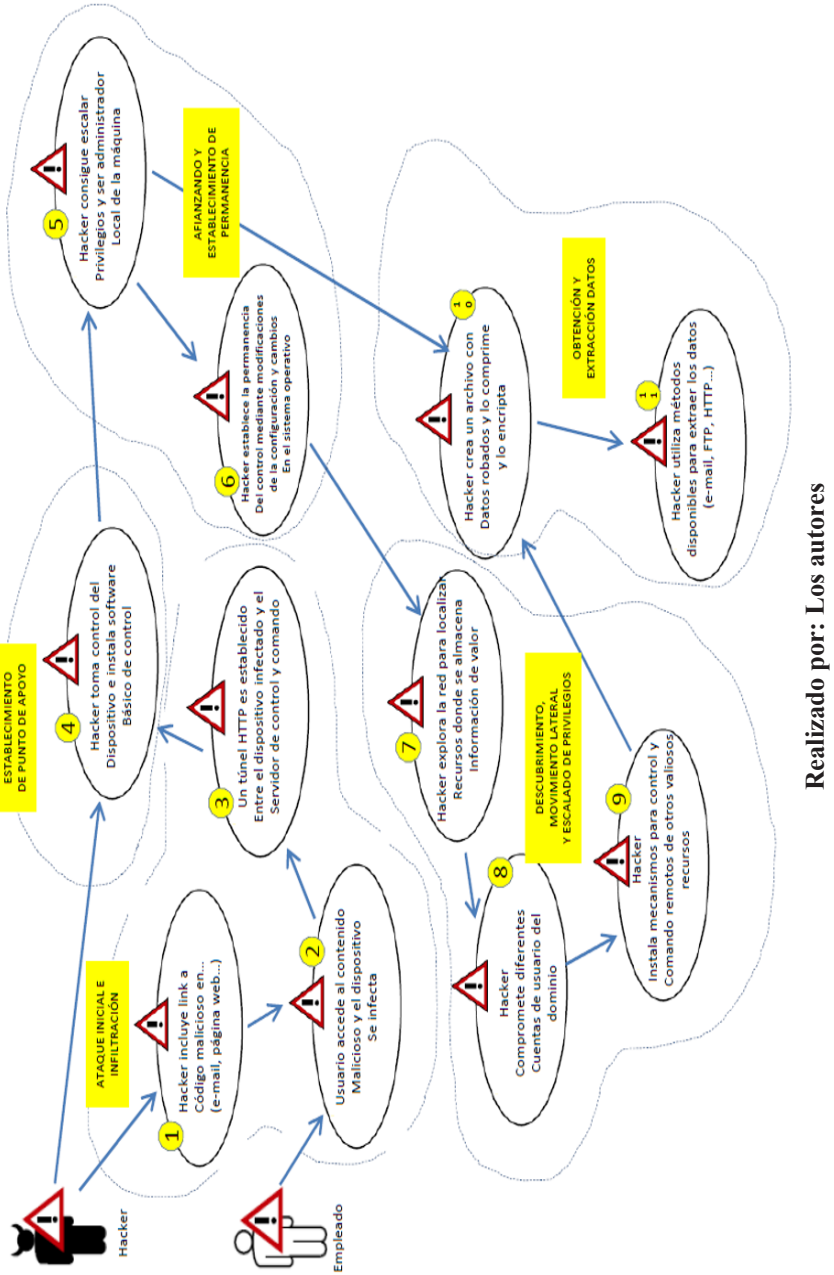
Obtención y extracción de datos

Una vez que los atacantes van obteniendo información de la institución, estos la irán agrupando en archivos comprimidos y debidamente cifrados almacenados en algún ordenador comprometido para posteriormente enviarlos al exterior haciendo uso de métodos utilizados por la institución (ejemplo: mails, internet).

Borrado de huellas

La eliminación de rastros o huellas es la fase final de un ataque informático, los intrusos por lo general eliminan todo tipo de pista que podría delatarlo durante el transcurso del ataque; los intrusos tratarán en lo máximo ir eliminando cada acción realizada para poder pasar por desapercibido. En la gráfica a continuación, se representan las amenazas detalladas anteriormente y las fases de ataque correspondientes. Las amenazas estarán representadas en el gráfico dentro de óvalos con la señal de peligro.

Figura 7. Esquema general del ataque



Realizado por: Los autores

Paso 4: Obteniendo la visión de conjunto

En el siguiente diagrama podemos sintetizar toda la información obtenida hasta el momento, y además observar desde una panorámica general, el cómo influyen diferentes individuos y como múltiples amenazas conceden una red que atenta directamente sobre los activos de la institución.

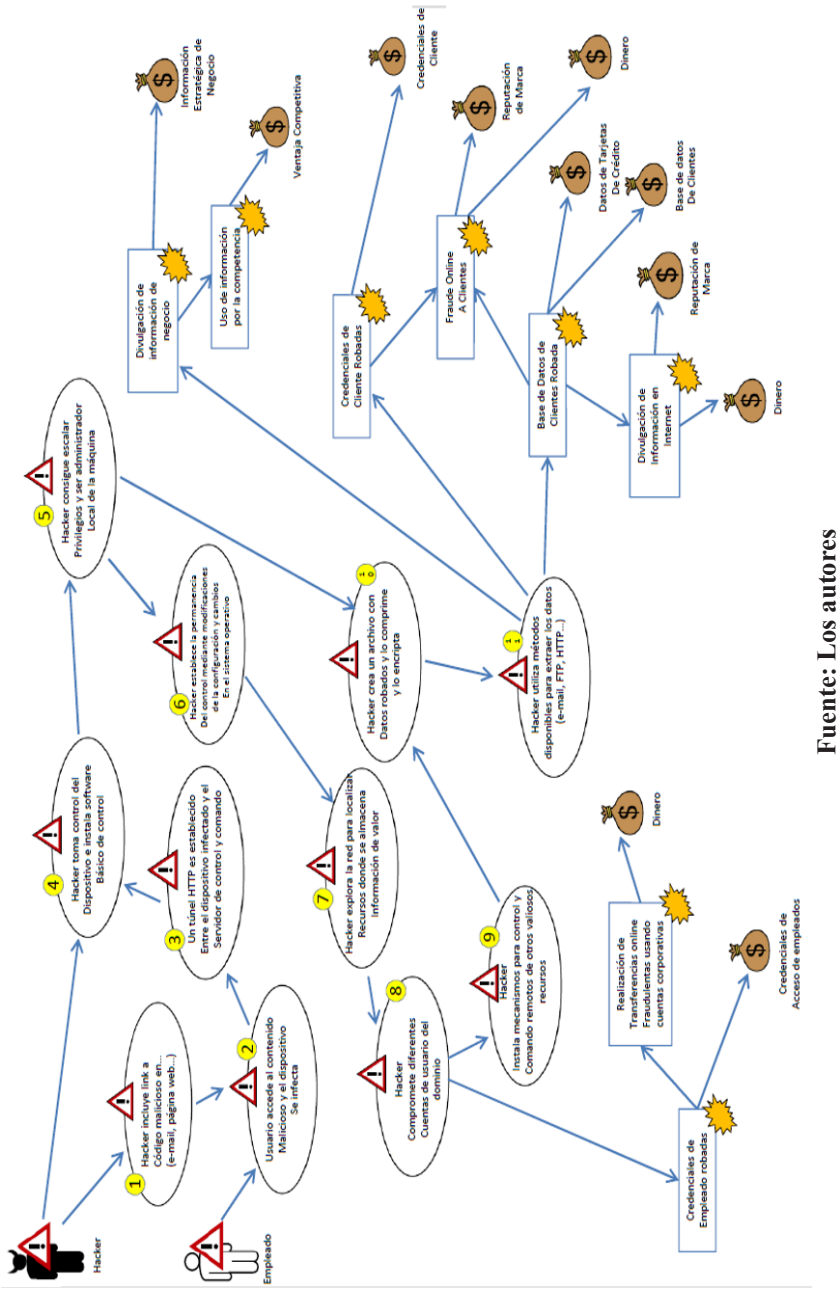


Figura 8. Visión general del ataque

Fuente: Los autores

Paso 5: Identificación de vulnerabilidades

Para la siguiente etapa optamos que, es necesaria la ayuda de personal calificado del departamento de tecnología de la institución y/o expertos en seguridad ya que serán parte del equipo de análisis. Este paso tiene como propósito identificar todas las vulnerabilidades técnicas o escenarios que permitan la ejecución de las amenazas identificadas en los pasos anteriores, tales amenazas estarán representadas en el diagrama.

Tenemos que tener en consideración que hay que identificar y registrar todas las vulnerabilidades potenciales independientemente de que estén o no incluidas en el caso de uso de la institución que estamos analizando. El objetivo de tal tarea, es proporcionar un escenario real de la situación y ayudar a documentar en etapas posteriores filtros y controles que serán necesarios implementar a la seguridad como también mejorar los controles ya implementados.

Entre las principales debilidades identificadas de nuestra institución en estudio tenemos:

- **La confianza de los usuarios para acceder a cualquier sitio web.** Esta vulnerabilidad en cualquier escenario es difícil de controlar especialmente si los atacantes son expertos en el uso de ingeniería social, incluso hasta personal experto en seguridad informática pueden ser víctimas de éstos si el engaño está bien tramado. Tengamos en consideración que los ataques dirigidos (APT) son efectuados por expertos calificados que diseñan

estrategias de intrusión a partir del análisis de la víctima.

- **Total acceso a la web y uso de correos electrónicos.** Mediante esta vía los atacantes son capaces de llegar a sus víctimas. Esta vulnerabilidad es muy difícil de evitar ya que no es un descuido o error por parte de los empleados ya que es una tarea justificada por las necesidades de trabajo.
- **Controles de antivirus y firewall del sistema deficientes.** En un ataque dirigido no hay protección, aun cuando el sistema conste con las últimas actualizaciones y parches de seguridad, ya que los softwares espías son diseñados para evadir cualquier tipo de filtro de seguridad y por ende sistemas antivirus.
- **Deficiente configuración de seguridad.** Una correcta configuración de seguridad de los equipos de comunicación puede ayudar a reducir los riesgos de una intrusión, como ejemplo podemos citar cuando los usuarios tienen permisos limitados en el sistema, entonces la propagación del software espía se torna dificultosa.
- **Deficiente monitorización de seguridad.** En todo sistema es muy fundamental la monitorización de la seguridad del mismo. Como ejemplo podemos suponer que cada vez que sea instalado un software o aplicación calificado como no oficial, en un equipo remoto activarse una alerta. Esta técnica ayudaría a frustrar un ataque y aplicar los correctivos correspondientes.
- **Débil segmentación de la red.** Una red segmentada correctamente

es una barrera de contención que al menos dificultará la expansión de una infección, ya que el software espía no tendrá total facilidad para expandirse por toda la red y por ende el intruso no tendrá acceso a información valiosa.

- **Políticas de contraseñas frágiles.** Por lo general los usuarios acostumbran a digitar contraseñas fáciles de descifrar, facilitando el trabajo de los atacantes para acceder a información de interés.
- **Información no cifrada.** La correcta protección de la información sensible mediante la aplicación de técnicas criptográficas robustas, en caso de un acceso no autorizado podría dificultar el éxito de un ataque informático.

Paso 6: Evaluación del grado de vulnerabilidad

En este paso será necesaria la realización de una valoración en conjunto con los miembros del equipo de análisis para determinar en qué medida las vulnerabilidades están controladas en la institución, esta tarea implicará la identificación de controles de seguridad (por ejemplo, el cifrado de bases de datos que contienen información sensible) y su evaluación de eficiencia. Este proceso permitirá tener una idea del grado de vulnerabilidad actual de la institución y la facilidad con que las múltiples amenazas se podrían materializar. Esta apreciación nos permitirá identificar las falencias y reducir los índices de vulnerabilidad.

RESULTADOS OBTENIDOS

Capítulo 5

RESULTADOS OBTENIDOS

Descripción de resultados

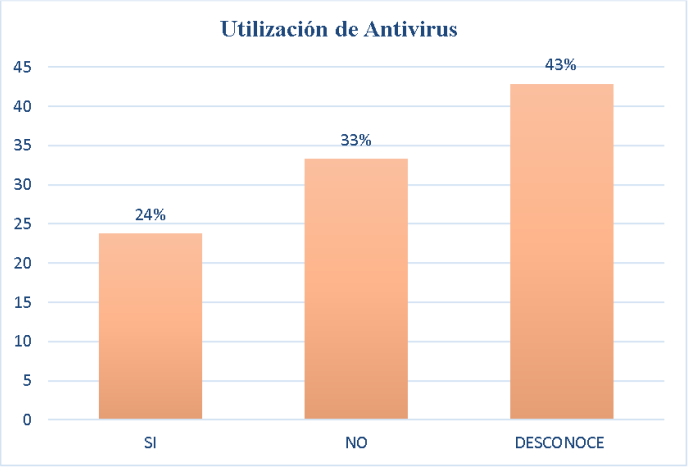
1. ¿El ordenador que utiliza tiene instalado antimalware?

Tabla 1: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
SI	5	24
NO	7	33
DESCONOCE	9	43
TOTAL	**21**	**100**

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 1: Descripción de Resultados



Fuente: Encuesta
Elaborado por: Los autores

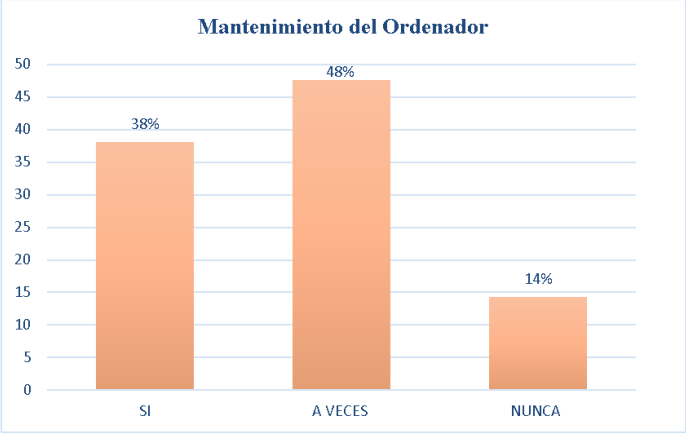
2. ¿Se le realiza un mantenimiento periódico al ordenador que Ud. utiliza por personal de soporte técnico de la institución?

Tabla 2: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
SI	8	38
A VECES	10	48
NUNCA	3	14
TOTAL	21	100

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 2: Descripción de Resultados



Fuente: Encuesta
Elaborado por: Los autores

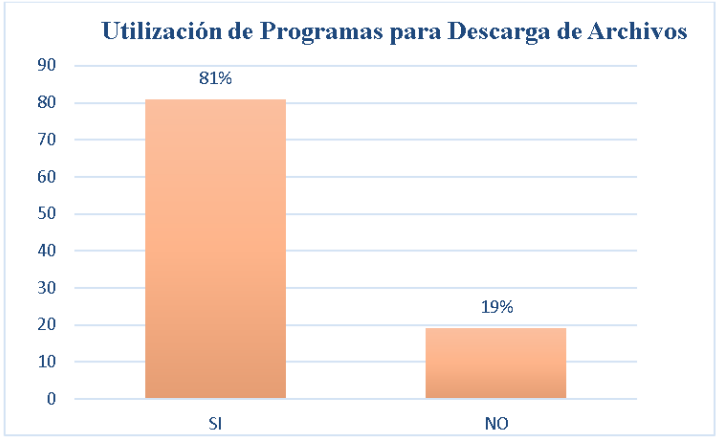
3. ¿Utiliza algún tipo de software para la descarga de archivos, música, películas, software, etc.?

Tabla 3: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
SI	17	81
NO	4	19
TOTAL	21	100

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 3: Descripción de Resultados



Fuente: Encuesta
Elaborado por: Los autores

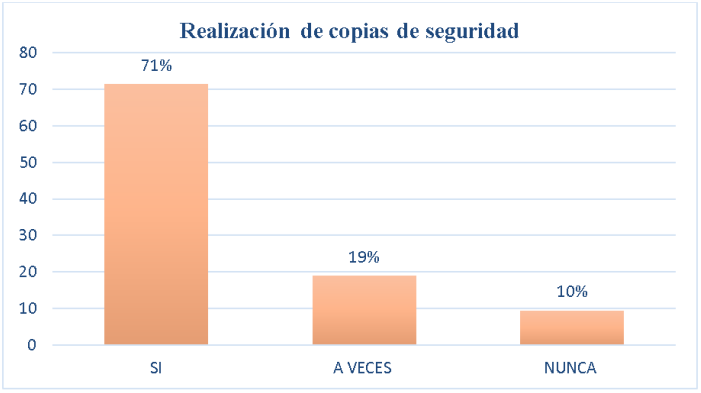
4. ¿Realiza copias de seguridad de los datos de la institución que Ud. maneja a diario en su entorno laboral?

Tabla 4: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
SI	15	71
A VECES	4	19
NUNCA	2	10
TOTAL	21	100

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 4: Descripción de Resultados



Fuente: Encuesta
Elaborado por: Los autores

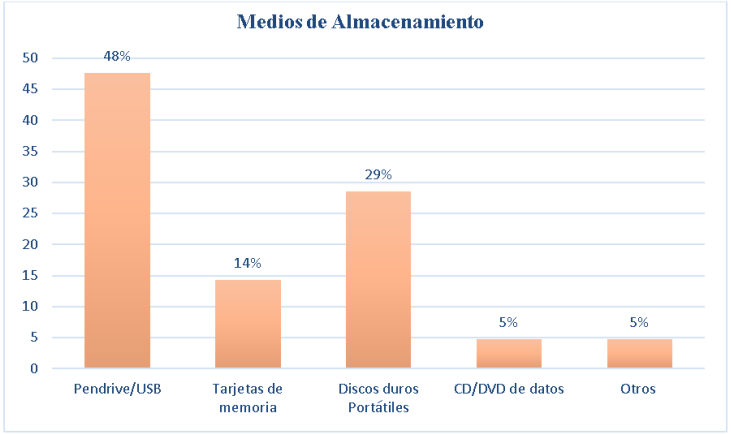
5. ¿Qué medios utiliza para el almacenamiento de la información y datos que Ud. maneja?

Tabla 5: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
Pendrive/USB	10	48
Tarjetas de memoria	3	14
Discos duros Portátiles	6	29
CD/DVD de datos	1	5
Otros	1	5
TOTAL	21	100

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 5: Descripción de los resultados



Fuente: Encuesta
Elaborado por: Los autores

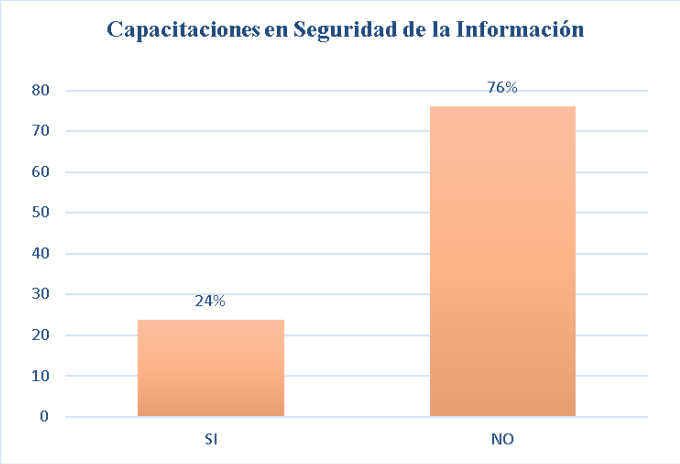
6. ¿Ha recibido capacitación acerca de la seguridad de la información?

Tabla 6: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
SI	5	24
NO	16	76
TOTAL	**21**	**100**

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 6: Descripción de Resultados



Fuente: Encuesta
Elaborado por: Los autores

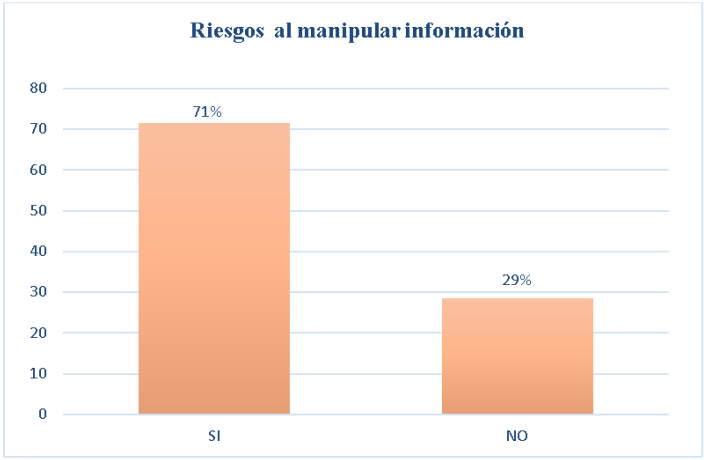
7. ¿Conoce los riesgos a los que se expondría la institución en caso de que llegase información confidencial a manos extrañas?

Tabla 7: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
SI	15	71
NO	6	29
TOTAL	**21**	**100**

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 7: Descripción de Resultados



Fuente: Encuesta
Elaborado por: Los autores

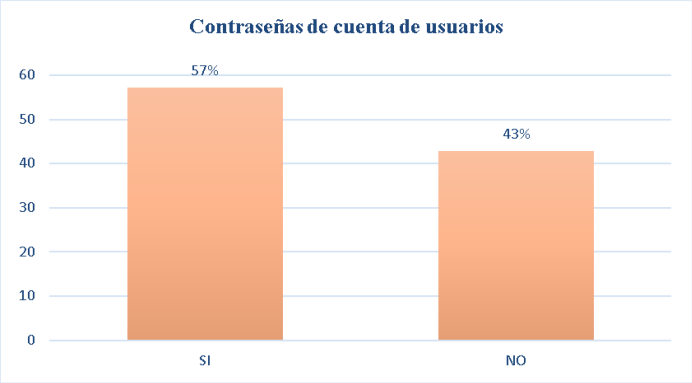
8. ¿Utiliza contraseña para ingresar a su cuenta de usuario?

Tabla 8: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
SI	12	57
NO	9	43
TOTAL	**21**	**100**

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 8: Descripción de Resultados



Fuente: Encuesta
Elaborado por: Los autores

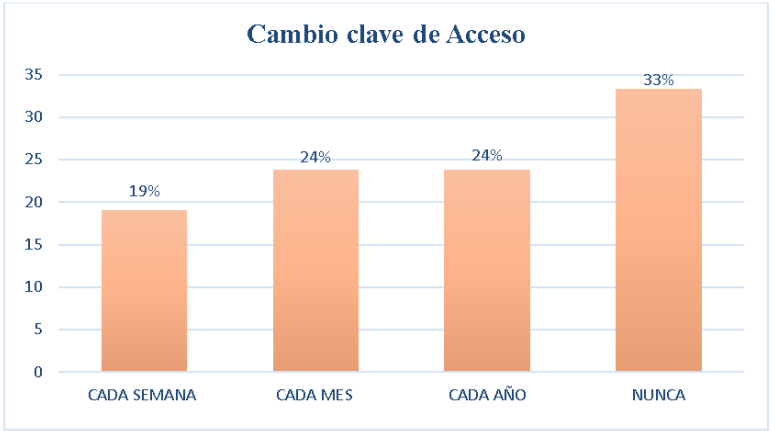
9. ¿Con qué frecuencia cambia su clave de acceso a sus cuentas de usuario?

Tabla 9: Descripción de los datos

OPCIONES	FRECUENCIA	PORCENTAJE
CADA SEMANA	4	19
CADA MES	5	24
CADA AÑO	5	24
NUNCA	7	33
TOTAL	**21**	**100**

Fuente: Encuesta
Elaborado por: Los autores

Gráfico 9: Descripción de Resultados



Fuente: Encuesta
Elaborado por: Los autores

Interpretación y discusión de resultados.

1. ¿El ordenador que utiliza tiene instalado antimalware?

Interpretación

De acuerdo con los resultados alcanzados del total de personas encuestadas hemos obtenido que el (24%) si hace uso del antivirus instalado en su ordenador, mientras que un (33%) de ellos no usa ningún tipo de antivirus y que el (43%) del personal que labora en la institución no tiene conocimiento acerca de antivirus.

Según nuestra interpretación podemos concluir que la mayoría de los encuestados en esta institución no conoce sobre la utilización de los antimalware.

2. ¿Se le realiza un mantenimiento periódico al ordenador que Ud. utiliza por personal de soporte técnico de la institución?

Interpretación

De las 21 personas encuestadas hemos obtenido que un (38%) afirma recibir frecuentemente el mantenimiento de su ordenador por parte del personal de soporte, mientras tanto un (48%) del personal opina que a veces reciben mantenimiento su computador y el (14%) restante opina que su ordenador nunca ha recibido mantenimiento por parte del personal de soporte.

En conclusión, podemos decir que la gran mayoría del personal encuestado necesita que sus ordenadores reciban el mantenimiento oportuno por parte del personal de soporte para así poder evitar cualquier tipo de contratiempos.

3. ¿Utiliza software para la descarga de archivos, música, películas, software, etc.?

Interpretación

Según la encuesta realizada en la institución se ha conseguido que el (81%) de las personas si utilizan programas para descargar archivos ya sea de música, películas, etc., mientras que el (19%) del personal restante no usan ningún tipo de programas para descargar.

Con los resultados finales de esta encuesta se puede apreciar que el 81% de las personas usan todo tipo de programas para descargar y esto conlleva a que existan riesgos de filtración de información.

4. ¿Realiza copias de seguridad de los datos de la institución que Ud. maneja a diario en su entorno laboral?

Interpretación

Como podemos observar en la descripción de los datos podemos decir que un (71%) del personal encuestado si realiza copias de seguridad de los datos de la institución, no obstante, el (19%) indica que solo a veces realiza copias de seguridad de los datos de la institución y el (10%) restante opina que nunca hacen copias de seguridad.

En conclusión, vemos que el mayor porcentaje del personal encuestado en el Ministerio de Inclusión Económica y Social de la ciudad de Babahoyo afirma realizar copias de seguridad de la información más relevante de la institución.

5. ¿Qué medios utiliza para el almacenamiento de la información y datos que Ud. maneja?

Interpretación

Según con la encuesta realizada podemos observar que el (48%) utiliza pen drive como medio de almacenamiento, un (14%) hace uso de las tarjetas de memoria, el (29%) utiliza los discos duros Portátiles, un (5%) usa como medio de almacenamiento para la información los CD/DVD de datos y un (5%) de ellos utilizan otros métodos de almacenamiento.

Como podemos apreciar, el pen drive es el medio de almacenamiento más utilizado por el personal que labora en esta institución.

6. ¿Ha recibido capacitación acerca de la seguridad de la información?

Interpretación

Del total de las personas encuetadas podemos observar que el (24%) afirma haber recibido capacitaciones sobre seguridad informática, por el contrario, el (76%) del personal encuestado opina que no ha recibido capacitación alguna a cerca de seguridad de la información.

De acuerdo con estos resultados nos podemos dar cuenta que el Ministerio de Inclusión Económica y Social necesita capacitar su personal de trabajo en cuanto a seguridad de la información.

7. ¿Conoce los riesgos a los que se expondría la institución en caso de que llegase información confidencial a manos extrañas?

Interpretación

Del total de las personas encuestadas observamos que el (71%)

opinaron que, si conocen los riesgos a los que se expondría la institución en el caso de que se extraiga información de gran importancia para la empresa, mientras que el otro (29%) restante no conoce los riesgos a los que se expondría la institución.

Según los resultados alcanzados de dicha encuesta se puede apreciar que el personal en su mayoría conoce y puede hacer algo por proteger la información confidencial de la institución.

8. ¿Utiliza contraseña para ingresar a su cuenta de usuario?

Interpretación

Según la encuesta realizadas al personal de la institución vemos que el (57%) opina que, si usa contraseñas para ingresar a su cuenta de usuario, mientras tanto el (43%) contestaron que no utilizan contraseñas.

El resultado que se obtuvo es que la mayoría de los encuestados hacen uso de contraseñas en sus cuentas de usuarios esto en cierta parte evita el robo de información por parte de personas malintencionadas.

9. ¿Con qué frecuencia cambia su clave de acceso a sus cuentas de usuario?

Interpretación

Mediante la encuesta realizada al personal observamos que un (19%) cambia su clave de acceso cada semana, un (24%) cambia su contraseña cada mes, un (24%) afirma cambiar su clave cada año y un (32%) opina que nunca cambia su contraseña.

En conclusión, podemos decir que el índice del porcentaje mayor es del 32% del personal que nunca cambia su contraseña y podemos

decir que debido a esto se pueden dar riesgos de pérdida de información o suplantación de identidad.

-ACERCA DE LOS AUTORES-

CÉSAR ALEJANDRO VALLEJO DE LA TORRE

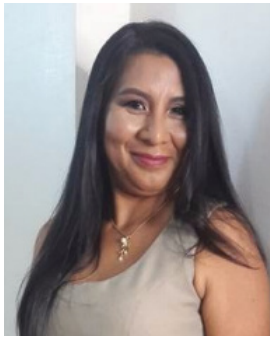
Profesional de la ciudad de Guayaquil, obtiene su título de Ingeniero en Sistemas Administrativos Computarizados en agosto del 2009, encaminado siempre en el ámbito profesional a las áreas de Sistemas y Administración, trabajó en el Sector Público, poniendo en práctica los conocimientos adquiridos. Además, continuando con sus aspiraciones profesionales, ingresó al programa de Maestría para obtener en el 2013 el título de Magister en Administración de Empresas con Mención en Sistemas de Información Empresarial. Actualmente es Profesor Titular Tiempo Completo en la Universidad de Guayaquil, Facultad de Ciencias Administrativas donde dicta las cátedras de E-Business y Administración de Redes Sociales. También realiza actividades de Investigación y Gestor de Practicas Pre Profesionales en la carrera de Ingeniería en Sistemas Administrativos Computarizados. @Cevade

PATRICIA MARÍA MARCILLO SÁNCHEZ

Es docente del área de Desarrollo de Sistemas y Gestora Social del Conocimiento en la Carrera de Ingeniería en Sistemas Administrativos Computarizados de la Universidad de Guayaquil. Su trabajo de Investigación está enfocado en el área Tecnología de Información y negocios.

Realizó los estudios de Licenciada en Sistemas de Información y Analista de Sistemas en Escuela Politécnica del Litoral (ESPOL). Máster en Administración de Empresas con Mención en Sistemas de Información Empresarial en la Facultad de Administración de la Universidad de Guayaquil. Maestrante de la Universidad Politécnica de Madrid España (UPM), Máster Universitario en Ciencias y Tecnologías de la Computación.

MARTHA VIVIANA UVIDIA VELEZ



- Profesora de Segunda Enseñanza Especialización Computación, graduada en la Universidad Técnica de Babahoyo.
- Licenciada en Ciencias de la Educación Especialización Computación, graduada en la Universidad Técnica de Babahoyo.
- Diploma Superior en Diseño de Proyectos, graduada en la Universidad Técnica de Babahoyo.
- Especialista en Liderazgo y Gerencia, graduada en la Universidad Técnica de Babahoyo.
- Magister en Gerencia de Proyectos Educativos y Sociales, graduada en la Universidad Técnica de Babahoyo.
- Magister en Educación Informática, graduada en la Universidad de Guayaquil.
- Docente en de la Facultad de Ciencias Agropecuarias en la Universidad Técnica de Babahoyo.

REFERENCIAS BIBLIOGRÁFICAS

- Alberto. (5 de Septiembre de 2009). Recuperado el 4 de Septiembre de 2014, de http://ataquesiformaticos.pdf
- ALEGSA.com.ar. (21 de Noviembre de 2015). DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA. Obtenido de DICCIONARIO DE INFORMÁTICA Y TECNOLOGÍA: http://www.alegsa.com.ar/Dic/vulnerabilidad.php
- Ataques en rdes LAN. (3 de Diciembre de 2015). Obtenido de Ataques en rdes LAN: https://sites.google.com/site/ataquesred/suplantacin-de-identidad/snooping-1
- Bermeo. (24 de Abril de 2012). Tesis Seguridad Informatica Dpto. Recuperado el 3 de Octubre de 2014, de Tesis Seguridad Informatica Dpto: http://TesisSeguridadInformaticaDpto.pdf
- Cas-Chile. (6 de Diciembre de 2015). Vulnerabilidades. Obtenido de Vulnerabilidades: http://www.bscconsultores.cl/descargas/B.2%20Vulnerabilidad.pdf
- César, T., & Álvaro, G. (22 de Noviembre de 2015). Sistemas Biométricos. Obtenido de Sistemas Biométricos: http://www.dsi.uclm.es/personal/MiguelFGraciani/mikicurri/Docencia/Bioinformatica/web_BIO/Documentacion/Trabajos/Biometria/Trabajo%20Biometria.pdf
- CoreOne. (16 de Noviembre de 2015). Disponibilidad de la Información. Obtenido de http://www.coreoneit.com/disponibilidad-de-la-informacion/

- Departamento de Seguridad Informática. (19 de Noviembre de 2015). Amenazas a la Seguridad de la Información. Obtenido de http://www.seguridadinformatica.unlu.edu.ar/?q=node/12
- EcuRed. (12 de Octubre de 2015). EcuRed conocimineto con todos y para todos. Obtenido de http://www.ecured.cu/Proteccion_contra_delitos_informaticos
- Encriptación de Datos. (20 de Noviembre de 2015). Encriptación de Datos. Obtenido de http://encripdedatos.blogspot.com/
- GITS Ciberseguridad. (20 de Noviembre de 2015). Seguridad Informática y Ciberseguridad. Obtenido de http://www.gitsinformatica.com/seguridad%20logica%20fisica.html
- Hacking Etico. (2 de diciembre de 2015). Hablemos de spoofing. Obtenido de http://hacking-etico.com/2010/08/26/hablemos-de-spoofing/
- Hernandez, M. (31 de Julio de 2006). Recuperado el 3 de Octubre de 2014, de http://TESISMariaGabrielaHernandezPinto.doc
- Hipertextual. (22 de Noviembre de 2015). Qué es la Ingeniería social y cómo estar prevenidos. Obtenido de Qué es la Ingeniería social y cómo estar prevenidos: http://hipertextual.com/archivo/2012/04/que-es-la-ingenieria-social-y-como-estar-prevenidos/
- HOSTALIA.com. (2 de Diciembre de 2015). XSS Attacks. Obtenido de XSS Attacks: http://pressroom.hostalia.com/wp-content/themes/hostalia_pressroom/images/cross-site-scripting-wp-hostalia.pdf

- In SlideShare. (12 de Noviembre de 2015). Integridad de la informacion. Obtenido de http://es.slideshare.net/CharlySantana1/integridad-de-la-informacion
- InfoSpyware. (2 de Diciembre de 2015). ¿Qué es el Phishing? Obtenido de ¿Qué es el Phishing?: https://www.infospyware.com/articulos/que-es-el-phishing/
- Jesús, J., & Rocío del Pilar, S. (21 de Noviembre de 2015). Firewalls personales. Obtenido de Firewalls personales: http://www.seguridad.unam.mx/descarga.dsc?arch=422
- Kimaldi. (21 de Noviembre de 2015). Área de conocimiento Biometria. Obtenido de Área de conocimiento Biometria: http://www.kimaldi.com/area_de_conocimiento/biometria/que_es_la_biometria
- Mgarzon. (9 de Junio de 2007). INTRODUCCION_ISO_17799. Recuperado el 2 de Octubre de 2014, de INTRODUCCION_ISO_17799: http://introduccion_iso_17799.pdf
- Mieres, J. (10 de Octubre de 2015). Obtenido de https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf
- MIES, i. (9 de Enero de 2013). ESTATUTO ORGANICO POR PROCESOS MIES. Recuperado el 3 de Septiembre de 2014, de ESTATUTO ORGANICO POR PROCESOS MIES: http://estatuto-organico-por-procesos-MIES-al-09-enero-2013-5.pdf
- Ministerio de Inclusion Economica y Social. (3 de Septiembre de 2014). Mision, Vision, Valores. Recuperado el 3 de Septiembre de 2014, de Mision, Vision, Valores: htpp://www.inclusion.gob.ec/misionvision/
- Phonet & Comunicaciones. (5 de Diciembre de 2015). Qué es un Backdoor. Obtenido de Qué es un Backdoor: http://www.phonet.mx/telecomunicaciones/post.php?p=qu-es-un-backdoor
- Quezada, A. E. (Octubre de 2013). Hacking con Kali Linux. Recuperado el 2 de Octubre de 2014, de Hacking con Kali Linux: http://www.reydes.com/d/?q=node/2
- Red Hat Enterprise Linux 4: Manual de seguridad. (6 de Diciembre de 2015). IDS basados en host. Obtenido de IDS basados en host: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-host.html
- Red Hat Enterprise Linux 4: Manual de seguridad. (6 de Diciembre de 2015). IDS basados en host. Obtenido de IDS basados en host: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-host.html
- Red Hat Enterprise Linux 4: Manual de seguridad. (6 de Diciembre de 2015). IDS basados en la red. Obtenido de IDS basados en la red: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-ids-net.html
- Red Hat Enterprise Linux 4: Manual de seguridad. (6 de Diciembre de 2015). Tipos de IDS. Obtenido de Tipos de IDS: http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/ch-detection.html

- Sebastián, S., & Nelson, S. (22 de Noviembre de 2015). Ing. Social e Ing. Social Inversa. Obtenido de Ing. Social e Ing. Social Inversa: http://inacap.serveftp.com/tic/Exposiciones_N1/Ingenieria%20social%20y%20social%20inversa.pdf
- Segu Info. (6 de Diciembre de 2015). Amenazas Humanas - Ex-Empleados. Obtenido de Amenazas Humanas - Ex-Empleados: http://www.segu-info.com.ar/amenazashumanas/exempleado.htm
- Segu Info. (6 de Diciembre de 2015). Amenazas Humanas - Personal Interno. Obtenido de Amenazas Humanas - Personal Interno: http://www.segu-info.com.ar/amenazashumanas/interno.htm
- Segu Info. (5 de Diciembre de 2015). Amenazas Lógicas - Tipos de Ataques - Ataques de Monitorización. Obtenido de Amenazas Lógicas - Tipos de Ataques - Ataques de Monitorización: http://www.segu-info.com.ar/ataques/ataques_monitorizacion.htm
- Segu Info. (6 de Diciembre de 2015). Detección de Intrusos en Tiempo Real. Obtenido de Detección de Intrusos en Tiempo Real: http://www.segu-info.com.ar/proteccion/deteccion.htm
- Segu Info. (7 de Diciembre de 2015). Seguridad Física. Obtenido de Seguridad Física: http://www.segu-info.com.ar/fisica/seguridadfisica.htm
- Seguridad Informatica. (6 de Diciembre de 2015). FRAUDES, ENGAÑOS Y EXTORSIONES. Obtenido

de FRAUDES, ENGAÑOS Y EXTORSIONES: https://seguridadinformaticaufps.wikispaces.com/FRAUDES,+ENGA%C3%91OS+Y+EXTORSIONES
- Sistemas de informacion. (21 de Noviembre de 2015). La Complejidad en un sistema de información. Obtenido de La Complejidad en un sistema de información.: http://silvosus.blogspot.com/2009/03/la-complejidad-en-un-sistema-de.html
- TechNet. (4 de Diciembre de 2015). Inyección de código SQL. Obtenido de Inyección de código SQL: https://technet.microsoft.com/es-es/library/ms161953(v=sql.105).aspx
- TechTarget. (16 de Noviembre de 2015). Privacidad de datos (privacidad de información): Definición. Obtenido de http://searchdatacenter.techtarget.com/es/definicion/Privacidad-de-datos-privacidad-de-informacion
- Universidad Nacional Autonoma de Mexico. (19 de Noviembre de 2015). Fundamentos de Seguridad Informática. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/AtaqPasivo.php
- Zona Virus. (2 de Diciembre de 2015). Que es el Spoofing. Obtenido de http://www.zonavirus.com/articulos/que-es-el-spoofing.asp

ANEXOS

tecnológicamente a través de la Plataforma de Dinero Electrónico (PDE) con el Banco Central del Ecuador.

Estos Participantes deberán suscribir el Acuerdo de Conexión (ACO) con el Banco Central del Ecuador en base a las normas jurídicas, técnicas, de calidad de servicio y de seguridades establecidas por el Consejo Nacional de Telecomunicaciones del Ecuador (CONATEL), que permita garantizar el normal funcionamiento del SDE y de la PDE. La participación de los Operadores de Servicio Móvil Avanzado (OSMAs) será regulada por el órgano competente de conformidad con la Ley de Telecomunicaciones vigente y demás normativa aplicable y controlada por la SUPERTEL.El Banco Central del Ecuador cuenta con el Permiso de Explotación de Servicios de Valor Agregado para la Operación del Sistema de Pagos y Transacciones Móviles. Para otros sistemas no indicados y que son parte de las Tecnologías de la Información y Comunicación, el Banco Central del Ecuador deberá obtener los permisos correspondientes.

1.15 MACRO AGENTES.- Son todas aquellas empresas, organizaciones e instituciones públicas y privadas; instituciones financieras y del sector financiero popular y solidario, que en su modelo de negocio requieran utilizar dinero electrónico para sus operaciones, mantengan una red de establecimientos de atención al cliente y que estén en capacidad de adquirir y distribuir el dinero electrónico por especies monetarias conforme la normativa que establezca el Organismo Regulatorio Competente. Estos Participantes deben controlar y supervisar la operación de los Centros de Transacción que se encuentren bajo su red afin de garantizar la calidad, seguridad y continuidad del servicio. El control de las operaciones de estos Participantes estará a cargo del Banco Central del Ecuador y se normarán con el REGLAMENTO DE PARTICIPANTES DEL SDE (RPDE) y el MANUAL DE PROCEDIMIENTO Y OPERACIÓN DEL SISTEMA DE DINERO ELECTRÓNICO (MPO).

1.16 CENTROS DE TRANSACCIÓN.- Serán los puntos de atención registrados por los Macro Agentes, que cumplan las condiciones establecidas en el REGLAMENTO DE PARTICIPANTES DEL SDE (RPDE) y el MANUAL DE PROCEDIMIENTO Y OPERACIÓN DEL SISTEMA DE DINERO ELECTRÓNICO (MPO), que proveerán de los servicios y productos del SDE a los Usuarios.

1.17 USUARIOS.- Son aquellas personas naturales o jurídicas, públicas o privadas, inscritas en el Sistema de Dinero Electrónico, que mantengan una CUENTA DE DINERO ELECTRÓNICO para realizar transacciones dentro del SDE a través de los MONEDEROS DE DINERO ELECTRÓNICO habilitados en los dispositivos autorizados y de acuerdo al REGLAMENTO DE PARTICIPANTES DEL SDE (RPDE).

1.18 CONVENIO DE PARTICIPACIÓN Y USO DE LA PDE PARA LA GESTIÓN COMERCIAL Y/O COBRANZA.- Documento mediante el cual

se habilita a los Usuarios Personas Jurídicas, para ofrecer una solución de cobro por sus productos y servicios usando la Plataforma de Dinero Electrónico.

1.19 MESAS DE AYUDA.- Son aquellos puntos de atención al público que se ubican dentro de un Centro de Transacción, que permitirán a los usuarios del Sistema de Dinero Electrónico solventar consultas y obtener ayuda.

Artículo 2.- El titular o portador de dinero electrónico, a través de los Macro Agentes autorizados en el SDE, podrá en cualquier momento solicitar el canje del valor nominal del dinero electrónico por especie monetaria física y viceversa.

Adicionalmente, los usuarios del Sistema de Dinero Electrónico podrán directamente a través de su monedero enviar y recibir transferencias desde y hacia su cuenta en el Sistema Financiero Nacional.

Artículo 3.- El saldo final diario de dinero electrónico del SDE se registrará en el pasivo del Balance General del Banco Central del Ecuador en contrapartida de las especies monetarias, los depósitos y las transferencias, en dólares de los Estados Unidos de América, recibidas por este concepto y que se registrarán en el activo del mismo Balance.

Artículo 4.- Condiciones de Ingreso de Participantes al Sistema de Dinero Electrónico.

4.1 Usuarios

4.1.1 Persona Natural

- Ciudadano o residente Ecuatoriano.
- Registrarse en línea a través del dispositivo móvil o de la página web del BCE.

4.1.2 Persona Jurídica

- Domiciliada en el Ecuador.
- Llenar el formulario de inscripción del Usuario y los documentos adicionales detallados en el Reglamento de Participantes.

4.2 Macro Agentes

4.2.1 Empresas Privadas, Públicas y Mixtas

- Formulario de inscripción del Macro Agente, suscrito por el Representante Legal y los documentos adicionales detallados en el Reglamento de Participantes.
- Funcionamiento mayor a dos años en el Ecuador, para empresas extranjeras.
- Más de dos años de funcionamiento para empresas nacionales.

- Capital pagado mínimo de cien mil dólares americanos (USD 100.000).
- Mantener puntos de atención en su cadena comercial.

4.2.2 Instituciones Públicas

- Formulario de inscripción del Macro Agente, suscrito por el Representante Legal y los documentos adicionales detallados en el Reglamento de Participantes.

4.2.3 Instituciones Financieras

- Formulario de inscripción del Macro Agente, suscrito por el Representante Legal y los documentos adicionales detallados en el Reglamento de Participantes.
- Encontrarse habilitado por el Banco Central del Ecuador en el Sistema Nacional de Pagos.

4.2.4 Organizaciones de la economía popular y solidaria

- Formulario de inscripción del Macro Agente, suscrito por el Representante Legal y los documentos adicionales detallados en el Reglamento de Participantes.
- Encontrarse habilitado por el Banco Central del Ecuador en el Sistema Nacional de Pagos.

4.3 Operadores Tecnológicos

- Ser una empresa domiciliada en el Ecuador que cuente con los permisos de operación vigentes.
- Contar con la infraestructura tecnológica y cobertura necesaria para que el dinero electrónico sea distribuido eficientemente y de manera segura por sus canales.
- Cumplir con las condiciones requeridas en el Acuerdo de Conexión entre el Banco Central del Ecuador y el Operador Tecnológico del ámbito correspondiente.

Artículo 5.- Obligaciones y responsabilidades de los Participantes del Sistema de Dinero Electrónico.

5.1 Del Banco Central del Ecuador como Administrador del Sistema de Dinero Electrónico

- Proporcionar el servicio de plataforma de dinero electrónico (PDE) a los participantes para efectuar las transacciones del SDE.
- Generar y mantener las normativas necesarias para el funcionamiento del SDE.

- Administrar el SDE conforme al Manual de Procedimiento y Operación del SDE (MPO) y el Reglamento de Participantes del SDE (RPDE) que expedirá la Gerencia General del Banco Central del Ecuador.
- Proporcionar a los Participantes toda la información necesaria para el correcto funcionamiento en el SDE.
- Calificar y autorizar las solicitudes de los Macro Agentes interesados en incorporarse al SDE, sobre la base de la normativa que al efecto expida la Gerencia General del Banco Central del Ecuador.
- Definir los montos máximos y mínimos que podrán transaccionar en cada caso de uso del SDE las personas jurídicas, sobre la base de lo dispuesto por la Junta de Política y Regulación Monetaria y Financiera.
- Definir y controlar el número máximo y mínimo de transacciones diarias y mensuales que podrán realizar los Participantes del SDE.
- Definir y controlar el número máximo y mínimo de monederos que se podrán asociar a las Cuentas de Dinero Electrónico de los Participantes del SDE.
- Establecer un esquema de segmentación para las CDE de los Participantes del SDE que permita establecer estadísticas.
- Crear cuentas de dinero electrónico a todos los Participantes del Sistema de Dinero Electrónico que cumplan los requisitos establecidos.
- Proporcionar información estadística del funcionamiento del SDE.
- Cumplir y hacer cumplir las disposiciones constantes en este Capítulo.
- Otras inherentes al mejoramiento del SDE.

5.2. De los Macro Agentes y los Centros de Transacción

- Cumplir todas las condiciones y requisitos para ser calificado como Macro Agente. Los requisitos estarán definidos en el Reglamento para Participantes del SDE (RPDE).
- Suscribir un Convenio de Adhesión para participar como Macro Agente del Sistema de Dinero Electrónico con el Banco Central del Ecuador.
- Garantizar eficiencia en la red de centros de transacción bajo su responsabilidad para las transacciones y operatividad del SDE.
- Entregar información clara y oportuna de las condiciones de acceso al servicio de dinero electrónico a los Usuarios del SDE.
- Entregar un servicio efectivo, seguro y disponible para los Usuarios del SDE.
- Participar en las iniciativas del Banco Central del Ecuador para impulsar el uso del SDE.
- Aceptar y aplicar las comisiones de operación y transacción establecidas por la Junta de Política y Regulación Monetaria y Financiera.
- Cumplir con los procedimientos establecidos por el Manual de Procedimiento y Operación del SDE (MPO).
- Cumplir con el control de las operaciones de los Centros de Transacción que se encuentren bajo su responsabilidad, con lo previsto en la Ley de Prevención, Detección y Erradicación del Delito de Lavado de Activos y Financiamiento de Delitos y las disposiciones relacionadas.

5.3 De los Operadores Tecnológicos

- Los Operadores Tecnológicos en el SDE firmarán un ACUERDO DE CONEXIÓN con el Banco Central del Ecuador y su operación será regulada conforme la Ley vigente establecida por el órgano regulador competente.
- Entregar un servicio con seguridad, continuidad, eficiencia, transparencia y equidad, que observe los estándares de calidad reconocidos por los organismos competentes.

5.4 De los Usuarios

- Brindar información fidedigna en el momento de activar su cuenta de dinero electrónico en el SDE y cuando sea requerida por el Macro Agente o por el Banco Central del Ecuador.
- Aceptar las tarifas de operación y transacción establecidas por la Junta de Política y Regulación Monetaria y Financiera.
- Responder por el uso y manejo de sus transacciones a través del SDE, en los términos previstos por la Ley de Prevención, Detección y Erradicación del Delito de Lavado de Activos y Financiamiento de Delitos y las disposiciones relacionadas.
- Cumplir con los procedimientos establecidos por el Manual de Procedimiento y Operación del SDE (MPO).

Artículo 6.- Derechos de los Usuarios.

- Acceso a la información necesaria para el correcto funcionamiento en el SDE.
- Contar con un servicio efectivo y disponible del SDE.
- Contar con un servicio de atención oportuna y eficiente.
- Los demás que se establecen en el marco normativo sobre la protección de los derechos de los usuarios.

CAPÍTULO II CUENTAS DE DINERO ELECTRÓNICO

Artículo 1.- Tipos de Cuentas de Dinero Electrónico

1.1 Por segregación de funciones y perfiles de los participantes del Sistema se definen los siguientes tipos de Cuentas de Dinero Electrónico:

- De Administrador
- De Macro Agente
- De UsuarioPersona Jurídica
- De UsuarioPersona Natural

1.2 La operación de las referidas cuentas se circunscribirá a las actividades inherentes y autorizadas a cada uno de los Participantes dentro del Sistema de Dinero Electrónico, establecidas en la normativa del SDE.

Dirección: Av. 10 de Agosto N11-409 y Briceño. Piso 8. Teléfono (593-2) 258 4949 / 295 4031. Fax: (593-2) 258 3068

CAPÍTULO III TRANSACCIONES Y CASOS DE USO

Artículo 1.-Transacciones

1.1 Dentro del Sistema de Dinero Electrónico se podrá operar mediante dispositivos electrónicos, electromecánicos, móviles o fijos, computadores, tarjetas inteligentes y otros dispositivos que vaya incorporando la tecnología y que se puedan integrar al SDE.

1.2 Los Usuarios del Sistema de Dinero Electrónico podrán realizar transacciones con los casos de uso disponibles en el Sistema.

Artículo 2.- Casos de Uso

A continuación se detallan los casos de uso disponibles para los Usuarios del SDE.

2.1 Activación de Cuenta de Dinero Electrónico (CDE)

Una persona natural o jurídica para activar una CDE deberá registrar sus datos en el Sistema de Dinero Electrónico mediante cualquier dispositivo activado con un Operador Tecnológico integrado al sistema o la página web del SDE.

Los Usuarios que deseen podrán llamar al Contact Center o acercarse a una Mesa de Ayuda del Sistema de Dinero Electrónico para recibir soporte para la Activación de su cuenta.

La CDE de una persona natural o jurídica tendrá asociada como identificador principal el número de cédula de identidad, cédula de identidad y ciudadanía o RUC respectivamente.

El Administrador del SDE no activará cuentas de usuarios que no se hayan autenticado debidamente, que tengan prohibiciones legales o estén dentro de las listas de control del Banco Central del Ecuador, en función de los resultados arrojados por el proceso de debida diligencia.

2.1.1 Habilitación de Monederos: El Usuario tendrá un monedero principal asociado a su CDE y podrá habilitar monederos adicionales, de acuerdo a lo establecido en el Reglamento de Participantes del SDE (RPDE).

El identificador del monedero de la CDE será el número de cédula de identidad o cédula de identidad y ciudadanía.

Dentro del Manual de Operación y Procedimientos (MPO) se establecen los mecanismos para habilitar y deshabilitar monederos de las Cuentas de Dinero Electrónico.

2.2 Desactivación de Cuenta de Dinero Electrónico

Todas las personas naturales o jurídicas usuarias del SDE, podrán el momento que lo requieran, desactivar de forma provisional o definitiva, su Cuenta de Dinero Electrónico para el efecto podrán llamar al Contact Center, acercarse a una Mesa de Ayuda o realizar la solicitud a través de la página web del Sistema de Dinero Electrónico y recibir soporte para la desactivación de su cuenta.

El Administrador del SDE, de considerarlo necesario, podrá iniciar de oficio el procedimiento para la desactivación provisional o definitiva en cualquiera de los casos previstosen el Reglamento de Participantes.

En caso de registrar saldos inmovilizados en las CDE se aplicará lo dispuesto en el Reglamento de Participantes del SDE.

2.2.1 Desactivación Provisional: Es la acción mediante la cual el Usuario Persona Natural o Jurídica, el Administrador del SDE o un tercero con interés legítimo desactiva una CDE, por un período de tiempo definido, pudiendo ésta ser reactivada o desactivada definitivamente.

2.2.2 Desactivación Definitiva: Es la acción mediante la cual el Usuario Persona Natural o Jurídica, el Administrador del SDE o un tercero con interés legítimo, desactiva una CDE de forma definitiva, perdiendo la prestación de servicios por parte del SDE.

2.3 Carga de Dinero Electrónico

El Usuario que tenga una Cuenta de Dinero Electrónico activa podrá en cualquiera de los Centros de Transacción autorizados por el BCE, cargar a su monedero dólares de los Estados Unidos de América.

La Carga de Dinero Electrónico a una CDE podrá tener los siguientes casos de uso:

- Carga de dólares de los Estados Unidos de América en un Centro de Transacción a una CDE de persona natural o jurídica.
- Servicio de uso de cajero automático asociado al SDE para Carga de dólares de los Estados Unidos de América a una CDE persona natural o jurídica.

2.4 Descarga de Dinero Electrónico

El Usuario que tiene una Cuenta de Dinero Electrónico activa, podrá en cualquiera de los Centros de Transacción autorizados por el BCE

descargar dólares de los Estados Unidos de América, desde su monedero.

Únicamente el Usuario registrado en el Monedero podrá realizar la descarga de dinero.

La Descarga de Dinero Electrónico de una CDE podrá tener los siguientes casos de uso:

- Descargade dólares de los Estados Unidos de Américaen un Centro de Transacción de una CDE de persona natural o jurídica.
- Servicio de uso de cajero automático asociado al SDE para Descargade dólares de los Estados Unidos de Américade una CDE de persona natural o jurídica.

2.5 Giro

Es la transacción que permite a un Usuario Persona Natural o Jurídica enviar dólares de los Estados Unidos de América desde su Cuenta de Dinero Electrónico a otra persona natural que no dispone de una Cuenta de Dinero Electrónico, para que lo retire en cualquier Centro de Transacción autorizado por el BCE. Así también, se considera como giro a aquellas transacciones que se realicen fuera del territorio ecuatoriano y se reciban en una Cuenta de Dinero Electrónico de un Usuario Persona Natural.

El giro de una CDE podrá tener los siguientes casos de uso:

- Giro nacional de una CDE de una persona natural o jurídica a una persona natural sin CDE.
- Giro del exterior a una CDE de persona natural.

2.6 Transferencia

El Usuario que mantenga una Cuenta de Dinero Electrónico activa, podrá transferir dólares de los Estados Unidos de América a cuentas del mismo Usuario en el sistema financiero nacional.

Todo usuario del sistema financiero nacional podrá transferir dólares de los Estados Unidos de América a una Cuenta de Dinero Electrónico activa de cualquier Usuario.

La transferencia de dinero electrónico de una CDE podrá tener los siguientes casos de uso:

- Transferencia desde una CDE de persona natural o jurídica a una cuenta de la misma persona natural o jurídica en el sistema financiero nacional.

- Transferencia desde una cuenta de persona natural o jurídica del sistema financiero nacional a una CDE activa de cualquier Usuario.

2.7 Solución de Pago

Es la transacción que permite, al Usuario que mantiene una Cuenta de Dinero Electrónico activa, pagar o enviar dólares de los Estados Unidos de América a un tercero que también tiene una Cuenta de Dinero Electrónico activa. Esta transacción se la podrá realizar mediante cualquier dispositivo registrado en el SDE.

La Solución de Pago de Dinero Electrónico podrá tener los siguientes casos de uso:

- Pago desde una CDE de persona natural o jurídica a otra CDE de personanatural o jurídica.
- Pago de impuestos y tasas al Gobierno Central (SRI, aduana, etc.), tasas e impuestos de los GADs, desde una CDE de persona natural o jurídica.

2.8 Solución de Cobro

El Usuario Persona Natural obligada a llevar contabilidad o la Persona Jurídica que mantengan Cuentas de Dinero Electrónico activas podrá gestionar cobros en línea o programados por los servicios o productos brindados, previa autorización del cliente.

La Solución de Cobro de Dinero Electrónico a una CDE podrá tener los siguientes casos de uso:

- Cobro autorizado programado a una CDE de persona natural o jurídica.
- Cobro en línea a una CDE de persona natural o jurídica.

Para disponer de esta transacción el Usuario Persona Jurídica deberá firmar un convenio con el Administrador del SDE.

2.9 Uso de la Plataforma para Gestión Comercial y/o Cobranza

Para disponer de esta transacción el Usuario Persona Jurídica deberá firmar un convenio con el Administrador del SDE.

2.10 Consulta de Saldo y Movimientos

El Usuario(a) que disponga de una CDE activa, podrá revisar en línea mediante la generación de un reporte, el detalle del saldo y movimientos de su cuenta y monederos, previa validación de identidad mediante el ingreso de su clave personal a través del dispositivo móvil, página web u otros mecanismos que en lo posterior implemente el SDE.

2.11 Cambio de parámetros de seguridad

El Usuario(a) que disponga de una CDE activa, podrá realizar el cambio de parámetros, como mecanismo de seguridad mediante su dispositivo móvil o la página web del SDE.

2.12 Certificado de CDE

El Usuario(a) que disponga de una CDE activa, podrá solicitar la certificación del saldo promedio, movimientos y propiedad de su Cuenta de Dinero Electrónico.

CAPÍTULO IV TARIFAS Y COMISIONES

Artículo 1.- TARIFAS DE LOS PARTICIPANTES DEL SISTEMA DE DINERO ELECTRÓNICO

Las tarifas por transacción y casos de uso del Sistema de Dinero Electrónico son las siguientes:

TARIFARIO DEL SISTEMA DE DINERO ELECTRONICO
(Los valores por tarifas incluyen IVA)

1. ACTIVACION DE CUENTA

Transacciones y casos de uso	Paga tarifa	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Tarifas (USD)
Activación de cuenta	N/A	N/A	N/A	0

2. CARGA DE DINERO ELECTRONICO*

Transacciones y caso de uso	Paga tarifa	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Tarifas (USD)
Carga de dinero electrónico en un centro de transacción a una CDE de persona natural	BCE	1	500	0
Carga de dinero electrónico en un centro de transacción a una CDE de persona jurídica	Persona Jurídica	1	500	0
Servicio de uso de cajero automático para carga de dinero electrónico a una CDE persona natural	BCE	5	500	0.1
Servicio de uso de cajero automático para carga de dinero electrónico a una CDE persona jurídica	Persona Jurídica	5	500	0.15

* El monto de la transacción dependerá de la categoría del centro de transacción o disponibilidad del cajero automático asociado

3. DESCARGA DE DINERO ELECTRONICO*

Transacciones y caso de uso	Paga tarifa	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Tarifas (USD)	
				De la 1era. hasta la 4ta. descarga realizada en ventanilla**	Desde la 5ta. descarga realizada en ventanilla**
Descarga de dinero físico en un centro de transacción de una CDE de persona natural	USUARIO	1	50	0	0.05
	USUARIO	51	200	0	0.1
	USUARIO	201	2500	0	0.15
Descarga de dinero físico en un centro de transacción de una CDE de persona jurídica	USUARIO	1	2500	0	0.15
Servicio de uso de cajero automático para Descarga de dinero electrónico de una CDE persona natural	USUARIO	5	500	0.1	
Servicio de uso de cajero automático para Descarga de dinero electrónico de una CDE persona jurídica	USUARIO	5	500	0.15	

* El monto de la transacción dependerá de la categoría del centro de transacción o disponibilidad del cajero automático asociado
** En un periodo mensual

4. TRANSFERENCIAS

Transacciones y caso de uso	Paga tarifa	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Tarifas (USD)
De una CDE de persona natural a una cuenta de la misma persona natural en el sistema financiero nacional	USUARIO QUE ENVÍA	1	100	0.05
	USUARIO QUE ENVÍA	101	2000	0.15
	USUARIO QUE ENVÍA	2001	9000	0.25
De una CDE de persona jurídica a una cuenta de la misma persona jurídica en el sistema financiero nacional	USUARIO QUE ENVÍA	1	Límite autorizado por el BCE	0.25
De una cuenta de persona natural en el sistema financiero nacional a una CDE de cualquier persona natural	USUARIO QUE RECIBE	1	9000	0
De una cuenta de persona jurídica en el sistema financiero nacional a una CDE de cualquier persona natural	USUARIO QUE RECIBE	1	9000	0
De una cuenta de persona jurídica en el sistema financiero nacional a una CDE de cualquier persona jurídica	USUARIO QUE RECIBE	1	Límite autorizado por el BCE	0.05
De una cuenta de persona natural en el sistema financiero nacional a una CDE de cualquier persona jurídica	USUARIO QUE RECIBE	1	Límite autorizado por el BCE	0.05

5. SOLUCION DE PAGOS

Transacciones y caso de uso	Paga tarifa	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Tarifas (USD)
Pago de una CDE de persona natural a otra CDE de persona natural	USUARIO QUE PAGA	0.01	0.99	0.015
	USUARIO QUE PAGA	1	10.99	0.02
	USUARIO QUE PAGA	11	50	0.04
	USUARIO QUE PAGA	51	300	0.06
	USUARIO QUE PAGA	301	2000	0.1
	USUARIO QUE PAGA	2001	9000	0.15
Pago de una CDE persona natural a una CDE de persona jurídica	USUARIO QUE COBRA	0.01	0.99	0.015
		1	10	0.02
		11	50	0.04
		51	300	0.06
		301	2000	0.1
		2001	9000	0.15
Pago de una CDE persona jurídica a una CDE de persona jurídica	USUARIO QUE PAGA	1	2000	0.1
		2001	Límite autorizado por el BCE	0.2
Pago de una CDE de persona jurídica a una CDE de persona natural	USUARIO QUE PAGA	1	9000	0.1
Pago de impuestos y tasas al Gobierno Central (SRI, aduana, etc.), tasas e impuestos de los GADs, desde una CDE de persona natural	USUARIO QUE PAGA	1	9000	0.05
Pago de impuestos y tasas al Gobierno Central (SRI, aduana, etc.), tasas e impuestos de los GADs, desde una CDE de persona jurídica	USUARIO QUE PAGA	1	Límite autorizado por el BCE	0.05

6. SOLUCION DE COBRO*

Transacciones y caso de uso	Paga tarifa	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Tarifas (USD)
Cobro en línea que realiza una persona jurídica a una CDE de persona natural	USUARIO QUE COBRA	0.1	0.99	0.015
		1	10	0.02
		11	50	0.04
		51	300	0.06
		301	2000	0.3
		2001	9000	0.35
Cobro en línea que realiza una persona jurídica a una CDE persona jurídica	USUARIO QUE COBRA	1	2000	0.3
		201	Límite autorizado por el BCE	0.3
Cobro autorizado programado que realiza una persona jurídica a una CDE de persona natural	USUARIO QUE COBRA	1	200	0.25
		201	9000	0.4
Cobro autorizado programado que realiza una persona jurídica a una CDE persona jurídica	USUARIO QUE COBRA	1	200	0.25
		201	Límite autorizado por el BCE	0.5

*Servicio de cobranza que aplica solo a personas jurídicas.

7. GIROS

Transacciones y caso de uso	Paga tarifa	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Tarifas (USD)
Giro nacional de una CDE de una persona natural o jurídica a una persona natural	USUARIO QUE ENVÍA	10	300	0.5
Recepción de un giro del exterior a una CDE de una persona natural (Remesas)*	BCE SBI	10	500	0
	BCE SBI	501	9000	0.05

*Remesas recibidas mediante los agentes autorizados del Banco Central del Ecuador

8. CONSULTA DE SALDO Y MOVIMIENTOS

Transacciones y caso de uso (mensual)	Paga tarifa	Numero mínimo de transacciones	Numero máximo de transacciones	Tarifas (USD)
Consulta de saldo y movimientos (5 movimientos ultimos) por dispositivo	USUARIO	1	10	0
	USUARIO	11	en adelante	0.05
Consulta de saldo y movimientos por web	BCE Web	1	ilimitado	0

9. CAMBIO DE PARÁMETROS DE SEGURIDAD

Transacciones y caso de uso (mensual)	Paga tarifa	Numero mínimo de transacciones	Numero máximo de transacciones	Tarifas (USD)
Cambio de clave por dispositivo móvil	USUARIO	1	2	0
	USUARIO	3	adelante	0.1
Cambio de PIN por la web	BCE	1	ilimitado	0

10. USO DE PLATAFORMA PARA GESTION COMERCIAL

Transacciones y caso de uso	Paga tarifa	Monto mínimo (USD)	Monto máximo (USD)	Tarifa (%)
Venta de productos y servicios de operadores tecnológicos*	PERSONA JURIDICA (vendedor)	3	Límite autorizado por el BCE	0.005
Otros productos y servicios	PERSONA JURIDICA (vendedor)	3	Límite autorizado por el BCE	0.2

* Estas transacciones están asociadas al Convenio de Participación y Uso de la Plataforma donde se estipula que los operadores tecnológicos (operadoras de servicio móvil avanzado y otros) no cobrarán ningún costo de conexión por estas transacciones.

11. CERTIFICACIÓN DE CDE

Transacciones y caso de uso	Paga tarifa	Cantidad mínima	Cantidad máxima	Tarifas (USD)
Certificado impreso	Usuario	1	en adelante	0.5

Artículo 2.- SISTEMA DE COMISIONES DE LOS PARTICIPANTES DEL SISTEMA DE DINERO ELECTRÓNICO

Las comisiones por transacción y casos de uso del Sistema de Dinero Electrónico son las siguientes:

COMISIONES DEL SISTEMA DE DINERO ELECTRONICO
(los valores por comisión incluyen IVA)

1. CARGA DE DINERO ELECTRONICO*

Transacciones y caso de uso	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Comisión que paga el BCE al macro agente (USD)	Comisión a entregar del macro agente al centro de transacción (USD)
Carga de dinero electrónico en un centro de transacción a una CDE de persona natural	1	500	0.05	0.04
Carga de dinero electrónico en un centro de transacción a una CDE de persona jurídica	1	500	0.05	0.04
Carga de dinero electrónico a través de un cajero automático a una CDE persona natural	5	500	0.1	NA
Carga de dinero electrónico a través de un cajero automático a una CDE persona jurídica	5	500	0.15	NA

* El monto de la transacción dependerá de la categoría del centro de transacción o disponibilidad del cajero automático asociado

2. DESCARGA DE DINERO ELECTRONICO*

Transacciones y caso de uso	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Comisión que paga el BCE al macro agente (USD)	Comisión a entregar del macro agente al centro de transacción (USD)
Descarga de dinero físico por ventanilla a persona natural	1	2500	0.06	0.05
Descarga de dinero físico por ventanilla a persona jurídica	1	2500	0.06	0.05
Descarga de dinero físico por cajero automático persona natural	5	500	0.1	NA
Descarga de dinero físico por cajero automático persona jurídica	5	500	0.15	NA

* El monto de la transacción dependerá de la categoría del centro de transacción o disponibilidad del cajero automático asociado

3. GIROS

Transacciones y caso de uso	Monto mínimo transacción (USD)	Monto máximo transacción (USD)	Comisión que paga el BCE al macro agente (USD)	Comisión a entregar del macro agente al centro de transacción (USD)
Giro nacional de una CDE de una persona natural o jurídica a una persona natural	10	300	0.4	0.3
Recepción de un giro del exterior a una CDE de una persona natural (remesa)*	10	500	0.4	0.3
	501	9000	0.5	0.4

*Remesas recibidas mediante los agentes autorizados del Banco Central del Ecuador

4. MESA DE AYUDA

Transacciones (mensuales) por cada mesa de ayuda	Cantidad mínima usuarios atendidos	Cantidad máxima usuarios atendidos*	Comisión que paga el BCE al macro agente (USD)	Comisión a entregar del macro agente al centro de transacción (USD)
Informativo y gestión a usuario por mesa de ayuda instalada en un centro de transacción	1	1000	0.1	NA
	1001	4000	0.08	NA
	4001	8000	0.05	NA

* Ocho mil es el número máximo de transacciones que por mesa de ayuda podrá realizar mensualmente bajo un estandar de calidad

5. CERTIFICACIÓN DE CDE

Transacciones y caso de uso	Cantidad mínima	Cantidad máxima	Comisión que paga el BCE al macro agente (USD)	Comisión a entregar del macro agente al centro de transacción (USD)
Certificado impreso	1	en adelante	0.4	NA

Dirección: Av. 10 de Agosto N11-409 y Briceño, Piso 8. Teléfono (593-2) 258 4949 / 295 4031. Fax: (593-2) 258 3068

CAPÍTULO V MONTOS TRANSACCIONALES MÁXIMOS Y MÍNIMOS APLICABLES A LAS CUENTAS DE DINERO ELECTRÓNICO

Artículo 1.- Los montos máximos y mínimos que se podrán transaccionar en las cuentas de Dinero Electrónico de los Participantes del SDE.

USUARIO		MONTO TRANSACCIONAL MENSUAL	
		MÍNIMO	MÁXIMO
PERSONA NATURAL		0	9000
PERSONA JURÍDICA O PERSONA NATURAL OBLIGADA A LLEVAR CONTABILIDAD	Segmento 5	0	20000
	Segmento 4	0	100000
	Segmento 3	0	500000
	Segmento 2	0	1000000
	Segmento 1	0	ilimitado
MACRO AGENTE		0	ilimitado
ADMINISTRADOR DEL SDE		0	ilimitado

Los detalles de transacción por cada caso de uso dentro de los rangos establecidos en esta Resolución serán definidos en el Reglamento de Participantes del SDE emitido por el Banco Central del Ecuador.

Artículo 2.- Los montos máximos y mínimos para realizar cargas y descargas en las cuentas de Dinero Electrónico de los Participantes del SDE son:

TRANSACCIÓN		MONTO DIARIO	
		Mínimo	Máximo
CARGA	Persona natural	1	500
	Persona jurídica	1	500
DESCARGA	Persona natural	1	2500
	Persona jurídica	1	2500

Los detalles de transacción por cada caso de uso dentro de los rangos establecidos en esta Resolución serán definidos en el Reglamento de Participantes del SDE emitido por el Banco Central del Ecuador.

DISPOSICIONES GENERALES

PRIMERA.- Corresponde a los Participantes asumir la responsabilidad por el origen y destino lícito de los fondos tramitados a través del SDE.

Sin perjuicio de la aplicación de controles operativos y monitoreo de las transacciones realizadas a través del SDE, el Banco Central del Ecuador no asumirá responsabilidad alguna sobre el origen o destino de las órdenes de pago y valores compensados y liquidados en el SDE.

SEGUNDA.- El Banco Central del Ecuador no asumirá responsabilidad alguna respecto de las fallas que presenten las plataformas tecnológicas de las instituciones participantes o respecto de los daños que éstas puedan sufrir por su participación en el SDE o en cualquier otro aspecto relacionado, así como los que se deriven de su uso inadecuado.

TERCERA.- El Banco Central del Ecuador podrásuspender temporalmente la intervención de cualquier Participante en el SDE ante un pronunciamiento público de autoridad competente, respecto de su operatividad.

CUARTA.- El incumplimiento de las disposiciones contempladas en estaResolución, por parte de los Participantes del SDE, será notificado por el Banco Central del Ecuador a los organismos de control.

QUINTA.- Facúltase al Gerente General del Banco Central del Ecuador a celebrar convenios de adhesión, acuerdos de conexión y demás documentos con personas naturales o jurídicas, públicas o privadas, que permitan estructurar y fortalecer el SDE.

SEXTA.- El Banco Central del Ecuador, con el fin de garantizar la sostenibilidad y seguridad del SDE, podrá deshabilitar casos de uso, así como aumentar las comisiones a pagar a los Macro Agentes hasta en un cincuenta por ciento (50%).

SÉPTIMA.- Las transacciones realizadas con dinero electrónico no son consideradas servicios financieros.

DISPOSICIÓN DEROGATORIA

Derógase la Regulación No. 055-2014 expedida por el Directorio del Banco Central del Ecuador el 28 de febrero de 2014, publicada en el Registro Oficial No. 208 de 20 de marzo de 2014; y,toda referencia a "Pago Móvil", "Dinero Móvil" y "Billetera Electrónica" y cualquier norma que se contraponga a la presente Resolución en la Codificación de Regulaciones del Directorio del Banco Central del Ecuador.

DISPOSICIÓN FINAL.- Esta resolución entrará en vigencia a partir de la fecha desu publicación en el Registro Oficial.

COMUNÍQUESE.-Dada en el Distrito Metropolitano de Quito, el 6 de noviembre de 2014.

EL PRESIDENTE,

Patricio Rivera Yánez

Proveyó y firmó la resolución que antecede el economista Patricio Rivera Yánez, Ministro Coordinador de Política Económica – Presidente de la Junta de Política y Regulación Monetaria y Financiera, en el Distrito Metropolitano de Quito el 6 de noviembre de 2014 - LO CERTIFICO.

EL SECRETARIO ADMINISTRATIVO ENCARGADO,

Ab. Ricardo Mateus Vásquez

Dirección: Av. 10 de Agosto N11-409 y Briceño, Piso 8. Teléfono (593-2) 258 4949 / 295 4031. Fax: (593-2) 258 3068

Centro de Investigación y Desarrollo Profesional

Generador de Conocimientos...

ISBN: 978-9942-792-39-6

Editorial