FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

SEGURIDAD EN LA RED EMPRESARIAL PRIVADA

JAVFRANK CONTRATISTAS S.A.C.

PRESENTADO POR

JOSÉ LUIS SALAZAR MELGAREJO

INFORME POR EXPERIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

LIMA – PERÚ

2016

USMP
UNIVERSIDAD DE SAN MARTIN DE PORRES
FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

SEGURIDAD EN LA RED EMPRESARIAL PRIVADA *JAVFRANK CONTRATISTAS S.A.C.*

INFORME POR EXPERIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

PRESENTADO POR

SALAZAR MELGAREJO, JOSÉ LUIS

LIMA – PERÚ

2016

ÍNDICE

RESUMEN

Actualmente, el uso de Internet se ha incrementado notablemente, a fin de mejorar la redacción, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información. Por tanto, es fundamental saber qué recursos de la empresa necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permite el acceso de la empresa a través de Internet. Para que un sistema sea seguro, deben identificarse las posibles amenazas, por lo tanto, conocer y prever el curso de acción de los virus. Asimismo, el objetivo de este informe es brindar una perspectiva general de las amenazas de los hackers, categorizarlas y dar una idea de cómo funciona para conocer la mejor forma de reducir el riesgo de intrusiones.

ABSTRACT

Currently, Internet use has increased dramatically in order to improve the wording, more and more companies allow their partners and suppliers access to their information systems. Therefore, it is essential to know what company resources need protection in order to control system access and the rights of users of the information system. The same procedures apply when access to the company via the Internet is allowed. For a system to be sure, they must identify possible threats, therefore, know and predict the course of action of the virus Also, the aim of this report is to provide an overview of threats from hackers, categorize and give an idea of how it works to know the best way to reduce the risk of intrusion.

INTRODUCCIÓN

Actualmente, la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles. Esto ha llevado a que muchas organizaciones hayan desarrollado documentos que orienten el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan.

De esta manera, las políticas de seguridad informática surgen como una herramienta para concientizar a los miembros de la empresa sobre la importancia y sensibilidad de la información. Las políticas de seguridad informática fijan los mecanismos y procedimientos que debemos adoptar para salvaguardar sus sistemas y la información que usamos.

El presente informe comprende cinco capítulos. El primero aborda la trayectoria profesional. En el segundo, se explica sobre la empresa donde se concretó el trabajo. El tercero corresponde a la descripción del proyecto. En el cuarto, se desarrolla el trabajo en sí, y en el quinto capítulo, se describe el desarrollo general del proyecto y sus implicancias.

CAPÍTULO I
TRAYECTORIA PROFESIONAL

M & M INGENIEROS S.R.LTDA.

Empresa de servicios de ingeniería con especialización en el rubro minero.

Fecha: 03/2000 – 03/2007

Especialista en sistemas:

- Responsable de los manuales de sistemas de la empresa.
- Responsable de las adquisiciones de hardware de la empresa.
- Responsable de los informes de sistemas.
- Implementación del área de informática.
- Implementación de la infraestructura informática.

Logros:

- Organización de la capacitación del personal de sistemas.
- Organización, preparación y revisión del plan de contingencia.
- Conocimiento en soluciones y herramientas de detección, diagnóstico y corrección de fallas a nivel hardware y software.

JAVFRANK S.A.C.

Empresa constructora en servicios para el rubro minero, ferroviario, gas y pesquero.

Fecha: 05/2007 – 07/20162

Asesor de sistemas:

- Responsable de la evaluación y selección de personal.
- Dirección y entrenamiento de personal para los procesos.
- Evaluación de la viabilidad técnica como la económica de los desarrollos de las aplicaciones que se han de ejecutar.

Logros:

- Organización de la formación del personal en seguridad.
- Control y desarrollo del sistema de seguridad informática.
- Cumplimiento de las normas de seguridad informática.
- Dirección, distribución de tareas y motivación del equipo para conseguir sus objetivos.
- Realización de informes de los procedimientos de seguridad.

CAPÍTULO II
EMPRESA DONDE SE REALIZÓ EL TRABAJO

2.1 Presentación: Javfrank Contratistas S.A.C.

La empresa del presente informe es JAVFRANK Contratistas S.A.C. empresa peruana del sector privado, con capitales íntegramente peruanos especializados en la fabricación, instalación y mantenimiento de diversos productos electromecánicos, eléctricos y electrónicos. Además, presta los servicios de consultoría empresarial.

Esta empresa tiene su sede en La Molina y cuenta con una filial, en Canto Grande.

2.2 Servicios

2.2.1 Mantenimiento:

- Mantenimiento de equipos de comunicación
- Mantenimiento de plantas industriales
- Mantenimiento de vías férreas

2.2.2 Fabricación:

- Tableros de distribución
- Tableros de transferencia automática
- Tableros de arrancadores de motores

2.2.3 Reparaciones:

- Sistemas hidráulicos
- Bombas centrífugas
- Grupos electrógenos

2.3 Organización:

La organización de JAVFRANK Contratistas S.A.C. tiene la siguiente estructura:

- Gerencia General
- Gerencia de Producción
- Gerencia de Proyectos
- Gerencia Financiera
- Gerencia de Marketing
- Gerencia de Logística

2.4 Principales clientes:

Los principales clientes de JAVFRANK Contratistas S.A.C. son:

- ABB (Asea Brown Boveri)
- Alfa Laval S.A.
- Alcon Ingenieros
- Bélgica Edificaciones S.A.
- Bticino
- Cohisa
- Compañía minera Antamina
- Compañía minera Yanacocha
- Compañía minera Barrick
- Ferrovías Central Andina
- Funsur S.A.
- Horse Power
- Kiev Asociados S.A.
- Laboratorios Abeefe
- Minsur S.A.

- Norandina
- Operandina S.A.
- Perufarma
- Phipsa contratistas
- Promotec contratistas generales
- Sergelco
- Solsa Contratistas S.A.
- 3C Contratistas S.A.

2.5 Misión

La empresa JAVFRANK Contratistas S.A.C. tiene definida su misión en los siguientes términos: “Ayudar a los clientes a resolver sus necesidades de Ingeniería más allá de sus obligaciones contractuales. Buscando la excelencia dentro de un marco de respeto y equidad en todos nuestros actos para maximizar el valor que damos a nuestros accionistas y empleados”.

2.6 Visión

La visión de JAVFRANK Contratistas S.A.C. está definida como: “Ser el principal referente de consultoría, servicios y proyectos y así logrando nuestra consolidación nacional. Y ser reconocida como una de las mejores empresas en el país por su excelencia en estándares de rentabilidad, productividad y responsabilidad”.

2.7 El Área de Sistemas

2.7.1 Área de sistemas

El Área de Sistemas en JAVFRANK Contratistas S.A.C. es el soporte de sus operaciones y de sus actividades empresariales. Está conformado por personal especializado, altamente calificado y cuenta con herramientas de tecnología avanzada, las cuales son manejadas por

recursos humanos capacitados y motivados, que colaboran bajo una cultura de cooperación y trabajo en equipo. El personal del Área de Sistemas trabaja con una mística de servicio, calidad, ética y eficiencia, desenvolviéndose en un ambiente que reconoce el mérito y propicia el desarrollo profesional especializado.

2.7.2 Funciones

En esta área, es donde he realizado mis labores profesionales, y mis principales funciones fueron:

1. Diseñar y desarrollar aplicaciones para las dependencias que lo solicitan.
2. Seleccionar, instalar y mantener el software y hardware.
3. Actualización mensual de nuestra Web: www.javfrank.com.
4. Asesoramiento en la compra de hardware y software para la empresa.
5. Desarrollar documentación específica con guías y recomendaciones para mejorar la seguridad.

CAPITULO III
DESCRIPCIÓN DEL PROYECTO

3.1 Enunciado

El presente informe de experiencia profesional titula “SEGURIDAD EN LA RED EMPRESARIAL PRIVADA JAVFRANK CONTRATISTAS S.A.”.

Este proyecto está enfocado al análisis y aplicación de herramientas de gestión de seguridad informática. Cuando se plantea, la seguridad, la idea es trazar todos los elementos que conforman nuestro sistema (hardware y software) y observar cuáles involucra más o menos riesgo, luego el resultado será un plan de seguridad cuyo objetivo es disminuir el riesgo total del sistema.

Pero, así como aumenta la accesibilidad, también aumenta el riesgo a que se expone la información importante, que se encuentra almacenada en la red. El desafío es garantizar que solamente las personas adecuadas y autorizadas tengan acceso a la información.

3.2 Antecedentes

La capacidad de utilizar redes empresariales para el comercio y la colaboración son el instrumento comercial clave que conlleva el gran surgimiento de las “empresas hiperconectadas”. Para satisfacer los requerimientos de las empresas, los niveles de gateway de las estaciones de trabajo y del servidor de las redes tienen que estar interconectadas lo que significa que la información importante de las empresas debe ahora residir en múltiples niveles de la red interna, donde cada nivel requiere su propia protección. Igualmente las amenazas a la red son más sofisticadas con técnicas de ataque que emplean diversos métodos para descubrir y aprovechar las vulnerabilidades de las redes, las que son más frecuentes. Por ejemplo, los virus, gusanos y caballos de troya, que a menudo se esconden dentro de los archivos o códigos de reprogramación, son capaces de autoreplicarse y autopropagarse para que los usuarios de las computadoras los esparzan fácilmente sin saberlo, que suma a la vulnerabilidad de los servidores para iniciar, transmitir y esparcir un ataque. Estas amenazas denominadas “combinadas” que están explícitamente diseñadas para aprovechar la vulnerabilidad de las tecnologías de la seguridad que utilizan métodos múltiples de ataque y autopropagación.

Debido a los múltiples niveles de vulnerabilidad de la red y la cantidad siempre creciente de técnicas de ataque, también aumentan los riesgos al bienestar corporativo. El impacto de los ataques a la red de la empresa puede variar desde consecuencias fáciles de cuantificar como las operaciones comerciales interrumpidas hasta pérdidas que son fáciles de calcular como los perjuicios al valor de las marcas. Los ataques a la red afectaron a la empresa de la siguiente manera:

- Interrupción de las operaciones comerciales. El tiempo fuera de servicio producido por un ataque ocasiona improductividad.

- Capacidad reducida para competir. La pérdida o hurto de la información produce graves consecuencias, incluso puede volver insostenible la posición de la empresa.

3.3 Finalidad

Contar con tecnologías de seguridad integrada para contribuir a la protección de la red de la empresa y la productividad de los empleados.

El concepto de seguridad integrada ha surgido para enfrentar los nuevos desafíos que afrontan las empresas en un mundo electrónico. La seguridad integrada combina múltiples tecnologías de seguridad junto con el cumplimiento de las políticas, el manejo de los clientes, el servicio, soporte y la investigación avanzada para obtener una completa protección. Al adoptar una estrategia integral que proporcione seguridad a las redes a nivel de los gateways, de los servidores y de las estaciones de trabajo, las organizaciones pueden reducir costos, mejorar la administrabilidad, aumentar el rendimiento, reforzar la seguridad y reducir el riesgo de exponerse a riesgos.

El enfoque de la seguridad integrada ofrece la más efectiva situación de seguridad en una proporción óptima de rentabilidad. La seguridad integrada utiliza en profundidad principios de protección y emplea funciones complementarias de seguridad en muchos niveles de la infraestructura de tecnologías de información.

Al continuar funciones múltiples, la seguridad integrada puede proteger más eficientemente contra una variedad de amenazas en todos los niveles para minimizar los ataques a las redes.

3.4 Alcance

El presente proyecto abarcará las diferentes áreas de la empresa, entre las más importantes se pueden mencionar:

• Finanzas
• Producción
• Logística
• Proyectos

3.5 Necesidad e importancia

El Plan de Sistemas fue considerado como uno de los más importantes proyectos, esto con la finalidad de:

• Eliminar o reducir los ataques a la red de la empresa.
• Proteger los sistemas operativos y las aplicaciones
• Políticas internas de seguridad.
• Capacitar y entrenar a los empleados.
• Utilizar sistemas de detección de intrusos
• Actualizar los servidores y aplicaciones.

3.6 Objetivos

3.6.1 Objetivo general

Establecer normas que minimicen los riesgos en la seguridad de la Red Empresarial Privada “Javfrank Contratistas S.A.C.”, estas incluyen horarios de funcionamiento, restricciones, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los empleados.

Asimismo, el objetivo de la seguridad informática es mantener la integridad, disponibilidad, privacidad, control y autenticidad de la información manejada por el usuario de la computadora.

3.6.2 Objetivos específicos

Conocer la importancia, los conceptos, metodologías, procesos de la seguridad informática y su implementación bajo un enfoque estratégico.

Sensibilizar a los profesionales del área de informática hacia la necesidad de proteger uno de los activos importantes de la empresa, la información.

Asegurar que solo las personas autorizadas tengan acceso a los recursos que se intercambian.

3.7 Factores críticos de éxito

Dentro de los factores críticos de éxito para llevar a cabo este proyecto se considera el siguiente:

3.7.1 Compromiso de los gerentes de la empresa

Dado que el proyecto se encuentra dentro del Plan de Sistemas, que juega un papel importante dentro de las expectativas con el fin de poder ser más competitivo y diferenciado, es que la Alta Dirección brindó lo necesario para el cumplimiento del mismo.

3.7.2 Definición de objetivos y alcances

Es importante tener claro los objetivos que se quieren lograr, y el alcance de los beneficios hacia donde está dirigido, esto con la finalidad

de comprometer a todo el personal con la meta establecida. Los empleados no siempre siguen y reconocen la importancia de las políticas de seguridad, la capacitación y entrenamiento que se les brinde, por lo tanto, no sería recomendable si ignoran las advertencias sobre el peligro de abrir los archivos adjuntos sospechosos del correo electrónico.

Los objetivos que se plantean son los siguientes:

1. Restringir el acceso a los programas de archivos.

2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas y los archivos que no correspondan.

3. Que la información transmitida sea recibida solo por el destinatario a quien ha sido enviada y no a otro.

4. Que la información recibida sea la misma que ha sido enviada.

5. Que se disponga de pasos alternativos de emergencia para la transmisión de información.

CAPÍTULO IV
TRABAJO REALIZADO

4.1 La Seguridad informática

4.1.1 Aspectos básicos de la seguridad informática

Un Sistema de Información es un elemento de gestión cada vez más importante, en la medida que la empresa incrementa su dependencia de ellos. Está compuesto por los recursos informáticos, considerados como el soporte informático y los activos de información, considerados como el contenido.

La seguridad informática permite compartir los Sistemas de Información de la empresa entre sus empleados, e incluso con terceros, pero garantizando su protección. La Seguridad tiene tres aspectos básicos que son esenciales para el crecimiento de la empresa y el cumplimiento de su legalidad vigente:

1. **Confidencialidad.** Protege los activos de información contra accesos no autorizados.

2. **Integridad.** Garantiza la exactitud de los activos de información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.
3. **Disponibilidad.** Asegura que los recursos informáticos y los activos de información pueden ser utilizados en la forma y el tiempo requerido.

Estos aspectos llevan implícitos los conceptos de propiedad, depósito y uso, de los recursos informáticos y activos de información, que posteriormente se desarrollaron.

4.1.2 Segregación de responsabilidades

Ciertas tareas (o áreas de responsabilidad) no pueden ser realizadas por la misma persona, a fin de reducir oportunidades de alteración no autorizada o mal uso de los sistemas de información. Para ello, es fundamental la segregación de responsabilidades, que minimiza el riesgo de mal uso accidental o deliberado del sistema de información. En algunas oportunidades, este control puede ser difícil de lograr, pero tiene que ser aplicado en la medida que sea factible.

Este control es particularmente importante para Sistemas que soporten aplicaciones más proclives al fraude. Incidentes de seguridad y procedimiento disciplinario. Un Incidente de seguridad es cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un sistema de información y/o pérdidas físicas o financieras para la empresa.

4.2 Políticas de seguridad

4.2.1 Análisis de riesgos

La seguridad informática tiene como objetivo el mantenimiento de la Confidencialidad, Integridad y disponibilidad de los Sistemas de Información. Es necesario identificar y controlar cualquier evento que pueda afectar negativamente a cualquiera de estos tres aspectos, así como definir e implantar las defensas necesarias para eliminar o reducir sus posibles consecuencias.

En un proceso de análisis de riesgos, se pueden establecer los siguientes componentes:

- **Sistema de información**. Son los recursos informáticos y activos de información de que dispone la empresa para su correcto funcionamiento y para la consecución de sus objetivos.

- **Amenaza**. Cualquier evento que, pueda provocar daños en los Sistemas de Información, produciendo a la empresa pérdidas materiales o financieras.

- **Vulnerabilidad**. Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas para causarles daño y producir pérdidas a la empresa.

- **Impacto**. Es la medición del daño que podría producir a la empresa la materialización de una amenaza sobre los Sistemas de Información.

- **Riesgo.** Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema de información, causando un impacto en la empresa.

- **Defensa**. Cualquier medio, físico o lógico, empleado para eliminar o reducir un riesgo.

En el proceso de Análisis de riesgos se pueden diferenciar:

1. La Evaluación de riesgos, orientada a determinar los Sistemas de Información que, en su conjunto o en cualquiera de sus partes, puedan verse afectados directa o indirectamente por amenazas, valorándose todos los riesgos y estableciendo sus distintos niveles a partir de las posibles amenazas, las vulnerabilidades existentes y el impacto que puedan causar a la empresa.

2. La Gestión de riesgos, que implica la identificación, selección, aprobación y manejo de las defensas (contra medidas) para eliminar, o reducir a niveles aceptables, los riesgos evaluados, con actuaciones tendentes a:
   - Reducir la posibilidad de que una amenaza ocurra
   - Limitar el impacto de una amenaza, si ésta se manifiesta
   - Reducir o eliminar una vulnerabilidad existente
   - Permitir la recuperación del impacto o su transferencia a terceros (contratación de seguros).

Un primer análisis de riesgos será mucho más costoso que los sucesivos. Puede requerir mucho tiempo y la participación de personal cualificado y especializado. El tiempo empleado está en proporción a los objetivos fijados y a su ámbito de cobertura.

Para resaltar la necesidad de sucesivos análisis de riesgos se deben tener en cuenta las siguientes consideraciones:

- Los elementos que componen los sistemas de información de la empresa están sometidos a constantes variaciones: nuevo personal informático, nuevas instalaciones, nuevos productos y aplicaciones, etc.
- Pueden aparecer nuevas amenazas o variar la probabilidad de que ocurra alguna de las existentes, afectando al posible impacto.

- Pueden aparecer nuevas vulnerabilidades o variar (o desaparecer) alguna de las existentes, creando o eliminando posibles amenazas.

En consecuencia, es necesario actualizar periódicamente, el análisis de riesgos tomando como base de partida el último realizado y las defensas implantadas hasta la fecha, por lo que los factores tiempo y medios necesarios para su realización serán menores.

El análisis de riesgos, además de centrarse en los sistemas de información existentes, es recomendable aplicarlo en el desarrollo de nuevos Sistemas, asegurándolos desde su creación.

El Área de sistemas de la empresa es responsable de definir y publicar, las Políticas de Seguridad como una firme declaración de intenciones, así como de divulgarlas en todo el ámbito de la empresa.

El conjunto de las Políticas de Seguridad debe establecer los criterios de protección en el ámbito de la empresa y servir de guía para la creación de las Normas de Seguridad.

4.2.2 Normas de seguridad informática

Basándose en las Políticas de seguridad, el Área de Sistemas publicó las Normas de seguridad, en las que se definió qué hay que proteger. Una norma debe ser breve, concisa y redactada en términos claros, y comprensibles por todos los empleados, y debe contener:

- Fecha de publicación.
- Fecha de efectividad o entrada en vigor.
- Fecha prevista de revisión o renovación.
- Si es aplicable a toda la empresa o a un ámbito más reducido.
- Si sustituye a una norma precedente o es nueva.

- Las normas son de cumplimiento obligatorio, por lo que deben ser divulgadas, de acuerdo con su ámbito de aplicación, a todos los empleados involucrados, incluido el personal directivo.

La responsabilidad del cumplimiento de las normas es de todos los empleados, pero especialmente del personal directivo que acumula a su responsabilidad como empleado, la de todos los empleados a los que dirige, coordina o supervisa.

El conjunto de todas las Normas de Seguridad debe cubrir la protección de todos los entornos de los Sistemas de información de la empresa.

4.2.3 Procedimientos de seguridad informática

Basándose en las Normas de Seguridad, y dependiendo del ámbito de aplicación, el Área de Sistemas creará los Procedimientos de Seguridad, en los que se describirá cómo proteger lo definido en las Normas y las personas o grupos responsables de la implementación, mantenimiento y el seguimiento para su cumplimiento, un procedimiento debe cubrir todo los aspectos descritos en la Norma que le soporta, siguiendo, de forma detallada y concreta todos los pasos en los que se estructura.

En un procedimiento se deben declarar todas las actividades que lo componen y definir todos los controles necesarios para cumplir con los requerimientos definidos en la Norma correspondiente. Adicionalmente, debe contener como información de control, al menos: o fecha de publicación; o fecha de efectividad o entrada en vigor; o fecha prevista de revisión o renovación, o responsable de su revisión y publicación, o relación de actividades, o responsables de cada actividad, o relación de controles por actividad, o valores críticos de los indicadores, o sustituye a un procedimiento anterior o es nuevo.

4.2.4 La Calidad en la seguridad

Teniendo en cuenta criterios de calidad, los procedimientos, y las actividades que lo componen, pueden estructurarse de tal manera que se podría definir un proceso por cada procedimiento.

En una segunda fase, las actividades que componen cada procedimiento (ahora proceso) deberían analizarse para evaluar si son, o no, automatizables. Posteriormente, se procedería a la automatización de las actividades que se hubieran declarado viables y a un segundo análisis y evaluación de las restantes actividades. De esta forma, paso a paso, se podría llegar a unos niveles de automatización que minimizarían la intervención humana, excepto en alguna toma de decisiones, obteniendo corno valor añadido la fiabilidad de estos procesos.

Siguiendo con los criterios de Calidad, los procesos deben ser revisados, periódicamente, como mejora continua, para la eliminación de defectos y la reducción del ciclo. Finalmente, resumir los objetivos de la aplicación de la Calidad en el Área de Seguridad:

- Incrementar la fiabilidad de los controles y sus indicadores, proporcionando alertas automáticas.
- Disminuir la intervención humana, con una reducción adicional del coste de personal.
- Reducir el ciclo de los procesos, permitiendo obtener información más actualizada.

4.3 Protección lógica

4.3.1 Información a los usuarios

Proteger los Activos de Información de la empresa para que sean siempre utilizados de forma autorizada, y solo por razones de negocio,

y. evitar acciones que puedan provocar su alteración, borrado o divulgación no autorizados, de forma accidental o intencionada.

El acceso de un usuario a los Sistemas de información de la empresa está basado, en cada caso, en la necesidad de uso por razones del negocio de la propia la empresa.

Los usuarios tienen que estar informados de los aspectos siguientes:

- Los Sistemas de la empresa solo pueden ser usados para fines del negocio de la propia empresa.
- El uso de los Sistemas para cualquier otro fin, de negocio o personal, debe ser previamente aprobado por el Área de Sistemas.
- El uso no autorizado de los Sistemas es una violación de los derechos de la empresa y se considera un abuso de confianza que debe ser sancionado.

Para ello, en la pantalla, inicial de conexión aparece una leyenda advirtiendo que “Los sistemas sólo pueden ser usados por razones de negocio u otros fines aprobados por la empresa”.

Deben quedar sujetos a revisión en todo momento, por el Área de Sistemas, las actividades realizadas por los usuarios, en los sistemas de la propia empresa, u otros ajenos a ella para los que tenga autorización de uso, y la utilización en ambos casos de los medios de almacenamiento correspondientes.

4.3.2 Identificación de usuarios

Es la clave que permite a un usuario acceder de forma individual a un Sistema de Información. Cada identificador de usuario está asignado a una persona, que será responsable de las actividades realizadas con él.

Generalmente, un identificador de usuario (junto con la contraseña o cualquier otro método de autenticación) se asigna a una persona para facilitarle el acceso a un único Sistema de Información, debiendo adquirir otros identificadores para el uso de otros Sistemas. Esto provoca la multiplicidad de identificadores y contraseñas, tanto más cuanto mayor sea el número de Sistemas existentes en la empresa y la necesidad de su utilización. Para resolver este posible problema, es recomendable:

- Definir y utilizar una nomenclatura estándar en la creación de identificadores, de forma que un usuario tenga el mismo identificador en todos los Sistemas que necesite utilizar.
- Instalar un Sistema de Control de accesos capaz de gestionar más de un Sistema de Información, con lo que el identificador de usuario (y la contraseña asociada) serían únicos y válidos para todos los Sistemas.
- Utilizar un método de Identificación única, que permita al usuario realizar los procesos de identificación y autenticación, una sola vez, en la primera conexión al sistema, pudiendo acceder, posteriormente, a cualquier otro sistema o servicio por propagación o conversión a los distintos identificadores de usuario y contraseña necesarios.

Adicionalmente, y dada la creciente necesidad de identificación (y autenticación) descritas, es posible dedicar un Sistema a las funciones de control de Seguridad, de modo que antes de permitir el acceso del usuario a cualquier Sistema de Información, se verifique una sola vez su identidad y autorizaciones de acceso. Este Sistema tendría que ser gestionado por el Administrador de Seguridad.

4.3.3 Identificador de usuario compartido

Hay casos en que un identificador de usuario proporciona acceso a determinadas funciones del sistema, que tienen que ser utilizadas

por un grupo de personas. En estos casos, el identificador de usuario puede ser compartido por el grupo bajo las condiciones siguientes:

- El identificador de usuario tiene que ser creado para el uso del grupo y no puede contener información individual, que el resto de los miembros del grupo no necesiten conocer.
- Siempre que sea posible, la contraseña no debe ser compartida, para permitir la identificación de la persona que lo está utilizando.
- Tiene que haber controles que eviten su uso no autorizado.

4.3.4 Autorización de usuarios

El acceso de cada usuario a los sistemas de la empresa tiene que ser aprobado previamente por el Área de Sistemas. Tiene que haber definido un procedimiento, automático o manual, para autorizar la inclusión de nuevos identificadores de usuarios en los Sistemas y que incluya la notificación al administrador responsable del usuario.

En caso de terminación de la necesidad de uso por razones de negocio o abandono de la empresa, tiene que haber definido un procedimiento, automático o manual, para la eliminación de identificadores de usuarios del sistema. El Administrador del usuario es responsable de comunicar a la Administración de Seguridad las condiciones de que son motivo de dicha eliminación.

Un identificador de usuario eliminado, no se volverá a asignar a ninguna otra persona en el futuro.

- **Revisión de vigencia.** Tiene que haber definido un proceso periódico para asegurar que no existen identificadores de usuario pertenecientes a empleados que hayan causado baja en la empresa.
  Este proceso puede utilizarse como base la comparación con alguna lista de empleados actualizada y servirá de salvaguarda en los casos

en que el procedimiento de eliminación de usuarios no haya sido aplicado correctamente.

Todos los identificadores de usuario, de empleados no activos en la empresa, encontrados en este proceso tienen que ser eliminados del Sistema, junto con todos sus derechos de accesos concedidos, y su baja comunicada al administrador responsable del empleado.

- **Usuarios inactivos.** Un identificador de usuario sin uso puede ser una vía de acceso no autorizado al sistema.

Tienen que establecerse controles para detectar identificadores de usuario que no hayan sido utilizados en los últimos 6 meses.

El proceso de detección de estos usuarios tiene que ser realizado, al menos, mensualmente, y su acceso al Sistema, desactivado.

La desactivación tiene que ser comunicada al Administrador responsable del empleado, advirtiéndole que en el plazo de un mes será eliminado el acceso al Sistema.

4.3.5 Revalidación anual de usuarios

Tiene que haber definido un procedimiento para la revalidación de usuarios, que deben ser analizados, al menos, anualmente.

Debe incluir el envío de la relación de usuarios a cada administrador que tiene empleados trabajando en el sistema, para que confirme si todos y cada uno ellos mantienen vigente la necesidad de uso por razones de negocio.

Las discrepancias deben ser comunicadas a la Administración de Seguridad para poder desactivar o eliminar a los usuarios.

4.3.6 Autenticación de usuarios

Con la autenticación del usuario se busca asegurar que el usuario es quien dice ser, cuando accede al Sistema.

En general, el proceso de autenticación de un usuario está basado en:

- Algo que sabe (contraseña).
- Algo que tiene (tarjeta, dispositivo, etc.).
- Algo que es (características biométricas).

La utilización de uno de los métodos anteriores se denomina Autenticación simple. Cuando los controles de acceso tienen que ser especialmente restrictivos, pueden combinarse más, métodos para eliminar, o al menos reducir, los riesgos de utilización no autorizada de un identificador de usuario. En este caso, la denominación es Autenticación Reforzada.

La mayoría de los Sistemas de Información utilizan la Autenticación Simple por contraseña.

4.3.7 Contraseñas (Passwords)

La contraseña de acceso es, hoy por hoy, la principal protección porque verifica inequívocamente, la identidad del usuario de un sistema.

Debe considerarse información clasificada las contraseñas, o cualquier otro método utilizado, de autenticación de usuario de acuerdo con el máximo nivel de información clasificada que el usuario pueda utilizar en el Sistema.

Para la protección de los activos de información de la empresa y la protección del propio usuario, la contraseña:

- Tiene que ser secreta y no compartida con nadie,
- No es visualizada en pantalla mientras se teclea, y
- No es almacenada en ningún tipo de Activo de Información.

Los sistemas operativos que incluyen algún Sistema de Control de Accesos, llevan rutinas de verificación de la calidad de la contraseña para evitar que pueda ser trivial o predecible. En cualquier caso, la contraseña debe disponer, como mínimo, de las características de calidad siguientes:

- Tener una longitud mínima de 6 caracteres; o tener al menos un carácter numérico y uno alfabético.
- No empezar ni terminar con un número; o no tener más de tres caracteres consecutivos idénticos, en cualquier posición, a los de una contraseña usada anteriormente.
- No tener más de dos caracteres iguales consecutivos.
- Debe cambiarse, al menos, cada 60 días para usuarios generales y cada 30 días para usuarios que tengan algún tipo de privilegio o autoridad.
- No ser reutilizada hasta después de, al menos, 12 cambios.
- No contener el identificador de usuario, como parte de la contraseña.

En muchos casos, sistemas operativos, productos informáticos o aplicaciones traen una contraseña ‘por defecto’ para ser usada durante su instalación. Sin excepción, estas contraseñas tienen que ser cambiadas, si técnicamente es posible, durante la primera utilización o a la mayor brevedad posible, en caso contrario.

Si, por razones de negocio, una persona tiene que utilizar sistemas ajenos a la empresa, no debe utilizar en ellos la misma contraseña utilizada en los sistemas internos de la empresa.

Si el nivel de Seguridad es inferior en aquellos, podría ser detectada y utilizada sin autorización en los sistemas de la empresa.

Para la restauración de contraseñas se tiene que haber definido e implantado un proceso para asegurar la restauración o cambio de contraseña, por pérdida u olvido de la anterior o cuando se sospeche que es conocida por otra persona.

El proceso debe incluir la identificación positiva del solicitante. Este proceso puede automatizarse para favorecer la gestión de la contraseña por el propio usuario.

Tanto la solicitud como la respuesta deben realizarse a través de medios seguros.

4.4 Activos de Información del Sistema objetivo

- Asegurar la integridad de los activos de Información del Sistema.

- Los activos de Información que están relacionados con el propio Sistema y sus funciones o con los productos que lo componen, se denominan Activos de Información del Sistema y su protección es responsabilidad, generalmente, de la Función de Sistemas de Información.

En este tipo de activos, cabe definir o destacar:

- Los programas de control del sistema y sus mecanismos de control de acceso.

- Los subsistemas, y productos soportados por Sistemas de Información, que formen parte del sistema operativo y sus funciones.

4.4.1 Activos sensibles del Sistema

Esta denominación afecta a los activos (datos y programas) que sean calificados sensibles por el Área de Sistemas.

Se entiende por dato sensible a cualquier activo de Información cuya modificación o alteración inadecuada o no autorizada podría afectar gravemente a la integridad de los Sistemas de información, sin ser prevenidos por los métodos habituales de control ni detectadas en un corto espacio de tiempo. Adicionalmente, este tipo de activos tienen que ser actualizados a través de un programa o transacción del propio sistema y nunca pueden ser modificados o actualizados directamente.

Un Programa Sensible es cualquier programa de utilidad ó del propio sistema, cuya utilización no autorizada o inadecuada podría comprometer la integridad de los Sistemas de Información. También se debe considerar sensible a cualquier programa de utilidad o del Sistema, que actualice Activos de Información definidos como datos sensibles. (ej.: cualquier programa de utilidad que analice el tráfico de red, ya sea local o extensa. Entre ellos los más conocidos por su denominación inglesa son: Spoofers, Sniffers, Trace Tools, etc.). Un programa sensible solo puede ser usado para los fines para los que fue creado, es decir, para el análisis, diagnóstico y resolución de problemas. Toda modificación, cambio o alteración de un Programa Sensible debe ser previamente autorizada.

Los Activos de Información sensibles no pueden ser, en ningún caso, accedidos públicamente y no puede haber usuarios que tengan acceso permanente a ellos, incluyendo las copias de respaldo. Los accesos temporales tienen que estar plenamente justificados y aprobados caso a caso. Todas, y cada una, de las actividades de uso y acceso realizadas por los usuarios, tienen que ser registradas y revisadas. Los accesos temporales tienen que ser eliminados, inmediatamente, después de terminar la necesidad de uso.

4.5 Activos de Información de usuario

Objetivo

Asegurar que cada activo de información de usuario está protegido, conforme a lo establecido por el Administrador y que tienen acceso los usuarios autorizados por él.

Los activos de Información que pertenecen a un usuario o grupo de usuarios, a una aplicación o son parte de alguna de ellas, se consideran Activos de Información de Usuario y la responsabilidad de requerir los controles adecuados para su protección es de los Administradores en las restantes funciones de la empresa.

Para este tipo de activos, tiene que establecerse una protección inicial por defecto que solo permita su acceso al Administrador del Activo. Todos los accesos concedidos, posteriormente, a otros usuarios tienen que estar explícitamente autorizados por el Administrador, independientemente de la clasificación o calificación del Activo.

El propietario del activo es responsable de establecer su protección y de los riesgos a que quede expuesto por una protección insuficiente. Tiene que asegurarse la integridad de todos los Activos de información de usuario.

4.5.1 Control de acceso público

Los activos de información de usuario no pueden tener ninguna opción que permita que sean accedidos públicamente. Si un usuario considera que alguno de sus activos tiene que ser accedido públicamente, debe:

- Certificar que el activo no contiene información clasificada, y
- Comunicarlo al Área de Sistemas.

La función de Sistemas de Información registrará como excepción todas estas solicitudes, advirtiendo al Administrador que su Activo va a ser accedido por todos los usuarios del sistema, incluidos usuarios externos si los hubiera.

Revisión periódica

La función de Sistemas de información tiene que comparar, al menos, mensualmente los activos de Información de usuario que pueden ser accedidos públicamente con la lista de excepciones autorizadas. Si durante esta comparación se encuentra algún Activo de Información de usuario con acceso público y no registrado, se restaurara la protección inicial por defecto, permitiendo su acceso sólo al Administrador.

La documentación relativa a estas revisiones debe ser guardada como documento auditable.

4.5.2 Activos sensibles de usuario

Esta denominación afecta a los activos (datos y programas) que sean calificados como sensibles por el administrador.

Dato sensible es cualquier activo de información cuya modificación o alteración inadecuada, podría causar graves pérdidas financieras a la empresa sin poder ser prevenidas por los métodos habituales de control ni detectadas en un corto espacio de tiempo.

Adicionalmente, este tipo de activos tienen que ser actualizados a través de un programa de aplicación y nunca pueden ser modificados o actualizados. (ej.: los datos que contengan las cuentas a pagar de la empresa o los que contengan la información de pagos a empleados y que no tengan suficiente verificación manual posterior).

Un Programa sensible es un programa de aplicación cuyo uso, modificación o alteración inadecuados o no autorizados podría causar graves pérdidas financieras a la empresa y no pueden ser prevenidas ni detectadas por los métodos habituales de control de aplicaciones.

También se debe considerar sensible a cualquier programa de aplicación que actualice Activos de Información definidos como datos sensibles. (ej.: un programa que cree instrumentos financieros negociables y que no tenga suficiente verificación manual posterior).

Toda modificación, cambio o alteración de un Programa Sensible debe ser verificada por un programador independiente del que la realizó, comprobando que se ha efectuado de acuerdo con los requerimientos del Administrador.

Los accesos temporales tienen que ser plenamente justificados y todas, y cada una de las actividades de acceso realizadas por los usuarios tienen que ser registradas y revisadas. Los accesos temporales tienen que ser eliminados inmediatamente después de determinar la necesidad de uso.

4.5.3 Protección en desarrollo

La protección de los activos de información generados o tratados por una aplicación, debe comenzar a planificarse durante el análisis y el desarrollo (o modificación) y consolidarse durante las pruebas previas a su paso al sistema de producción.

Estos requerimientos son aplicables a los desarrollos realizados en la propia empresa o encargados a terceras partes, y deben permanecer vigentes en las posteriores modificaciones por mantenimiento de la aplicación. Simultáneamente con el desarrollo, o modificaciones de

mantenimiento, deben crearse datos de prueba que verifiquen todas las alternativas de cada uno de los programas que componen la aplicación.

Nunca deben ser utilizados datos reales en pruebas, porque no se comprobarán todas las condiciones existentes en los programas y porque su utilización puede comprometer la confidencialidad, integridad y disponibilidad de los Activos reales de producción: Estos datos de prueba deben ser guardados durante la vida de la aplicación y actualizados cada vez que se realice alguna modificación en la aplicación que así lo aconseje.

Separación de los Sistemas de Desarrollo y Producción

Las actividades de desarrollo y prueba pueden causar cambios no deseados en activos de información de producción si comparten el mismo sistema o entorno operativo.

Para evitarlo, o al menos minimizarlo, hay que aislar, tanto como sea posible, los sistemas de desarrollo y prueba de los operacionales o de producción. Todos los desarrollos de aplicaciones, y sus posteriores modificaciones por mantenimiento, tienen que realizarse al margen del entorno operacional o de producción.

Dentro del área de gestión de cambios, el paso de aplicaciones desde el entorno de desarrollo y prueba al entorno operacional o de producción, no puede ser realizada por las mismas personas que desarrollan o mantienen las aplicaciones.

4.5.4 Protección de terminales

Todo usuario es responsable de proteger el terminal que le ha sido asignado, y colaborar en la protección de cualquier otro terminal de la empresa, para evitar que sea robado o dañado (total o

parcialmente), usada la información que contiene y utilizado el sistema al que está conectado.

Durante la jornada laboral, en ausencias que excedan de un tiempo razonable (más de 30 minutos), es necesario bloquear el terminal. Para ello utilizar la cerradura física (si la tiene) y guardar la llave en lugar seguro o utilizar productos de bloqueo y arranque mediante contraseña.

Como protección adicional, si se trabaja en un despachó que disponga de cerradura, hay que cerrarlo con llave.

Al finalizar la jornada laboral, utilizar los mecanismos de bloqueo físicos o lógicos descritos en el punto anterior. Los despachos deben permanecer abiertos por razones de higiene (limpieza diaria) y seguridad de las personas (si se produce un foco de incendio, inundación, etc. es necesario extinguirlo lo antes posible para evitar su propagación). Si el terminal es portátil, hay que guardarlo bajo llave o llevarlo consigo.

Durante los viajes (si se dispone de un terminal portátil), hay que usar mecanismos físicos o lógicos de bloqueo. No dejarlo nunca a la vista en el coche o en la habitación del hotel. No dejarlo al personal del hotel ni facturarlo como equipaje en aeropuertos o estaciones. Siempre que se pueda, el portátil debe permanecer en poder del empleado permanentemente.

Revisión Periódica

El administrador de seguridad tiene que revisar, al menos mensualmente, que los terminales están convenientemente protegidos y que a través de ellos no pueden ser accedidos los activos de Información contenidos en el terminal ni los Activos de Información contenidos en el Sistema o Servidor de una red de área local (LAN) al que pueda conectarse.

La documentación relativa a estas revisiones debe ser guardada como documento auditable.

4.5.5 Cifrado o criptografiado

Cuando el acceso físico o lógico a los activos de información no pueda ser controlado o, por su especial sensibilidad o confidencialidad, requieran medidas adicionales de seguridad, la información tiene que cifrarse de forma que quede ilegible y no pueda ser procesado por ningún usuario o persona no autorizada.

Un Activo de información cifrado, para su almacenamiento o envío, mantiene el mismo nivel de clasificación y tiene que ser protegido como el activo original.

Claves de cifrado

Las Claves de cifrado es una serie de caracteres usados para la codificación de los activos, sin la cual no serán legibles ni podrán ser procesados.

Protección de las claves de cifrado

Para la protección de las claves de cifrado tienen que haber definidos e implantados los controles siguientes:

- El uso de las claves debe estar restringido a personas.
- Usuarios con necesidad de conocerlas por motivos de trabajo; o la gestión y distribución de las claves debe estar restringido a las personas o usuarios autorizados a realizar las funciones de cifrado.
- La autorización de uso de las claves debe ser aprobada por el Administrador de la información de lo que se va cifrar o descifrar.

- El usuario de esta información puede delegar formalmente en el responsable del servicio de cifrado, si lo hubiera, la gestión y aprobación de las claves; el método usado para distribución de las claves tiene que poder asegurar que son recibidas por el destinatario, y solo por él.
- La clave de cifrado tiene que ser transmitida por un conducto distinto al del Activo, cuando este se transmita cifrado.
- Cuando el cifrado y descifrado no se realice por medio de programas, los Recursos Informáticos tienen que estar protegidos en un Área de Acceso Restringido (AAR).

Responsabilidades

El Administrador de la información cifrada, o los responsables del servicio de cifrado por delegación, tienen que asegurar que existen controles, para el cifrado y la protección de las claves, y son eficaces. Para poder demostrarlo deben guardar toda la documentación relativa al proceso y sus controles como documentos auditables.

4.5.6 Virus Informáticos y otros Códigos Dañinos

Son aquellos programas, rutinas o instrucciones desarrollados para provocar la destrucción o alteración de activos de Información, en el Sistema.

Existen distintos tipos de código dañino y que, dependiendo de la característica que lo diferencia, se describen a continuación:

- Virus Informáticos, el código que es capaz de generar copias de si mismo en programas distintos al que ocupa.
- Gusanos (Worms), el código que absorbe recursos del Sistema, de forma creciente, hasta que lo bloquea por saturación.

- Caballos de Troya (Trojan Horses), el programa de uso autorizado que contiene código dañino. Cuando este programa comienza a ejecutarse, el código dañino toma el control.
- Bombas Lógicas (Logic Bombs). El código que se ejecuta al producirse un hecho predeterminado, ej.: una determinada fecha, un número de encendidos del sistema, determinada secuencia de teclas, etc.

El más extendido es el virus informático que suele contener varias de las características descritas A partir de ahora, por simplificar, se empleará la palabra Virus para referirse genéricamente a cualquier forma o tipo de código dañino.

Existen, en el mercado, programas antivirus que detectan la presencia de virus y pueden eliminarlos. Estos programas van siendo actualizados de forma periódica, incorporando protección contra nuevos virus aparecidos. No obstante, siempre se estará expuesto a los virus que no hayan sido incluidos en los programas anti-virus, pero el riesgo será mucho mayor si no utilizamos ningún método de prevención y/o eliminación.

Protección en LAN y PC

La Infección por virus se produce por la ejecución de un programa contaminado o el arranque del sistema desde un disco removible contaminado.

Se pueden dividir en dos grandes grupos:

- Virus de programa, que infectan a ficheros ejecutables (extensiones EXE, COM, SYS, OVL, OVR, etc.).
- Virus de sector de arranque, que contaminan el sector de arranque de discos removibles y discos fijos.

Para eliminar, o al menos minimizar, la infección por virus deben tenerse en cuenta las siguientes consideraciones:

- Establecer la prohibición de uso de productos sin licencia, no autorizados por la empresa o adquiridos de fuentes sin garantía.

- Verificar con programas antivirus, antes de ser utilizado en el sistema, cualquier disco removible o fichero recibido que provenga de otro usuario, ya sea de la empresa o del exterior.

- Mantener un producto anti-virus residente de forma permanente en el sistema; actualizar el producto anti-virus utilizado, cada vez que se sepa que existe una versión más moderna que la que se está usando.

- Realizar periódicamente copias de respaldo.

Cualquier infección detectada en el transcurso de las verificaciones o revisiones descritas, tiene que ser notificada al Área de Sistemas, para el aislamiento de los sistemas afectados, el análisis del virus y, si fuera necesario, su posterior inclusión en el anti-virus.

Adicionalmente, debe haber una protección para la conexión de sistemas a una red de área local (LAN), que garantice que ningún usuario pueda introducir programas o datos infectados en el servidor o en el sistema de cualquier otro usuario de la LAN.

Está prohibido, propagar conscientemente programas o datos infectados por virus dentro de, o desde, la empresa.

La responsabilidad de la utilización de anti-virus y la salvaguarda de las estaciones de trabajo (terminales) es del usuario final, pero el Área de

Sistemas debe darle soporte para poder actualizar los programas anti-virus y canalizar las notificaciones de existencia de virus.

Protección en Sistemas Corporativos

La conexión de sistemas y redes a otros sistemas o redes puede suponer un grave riesgo para toda la red, los sistemas conectados a ella y los Activos de Información contenidos en los sistemas.
Deben controlarse todas las transferencias de Activos recibidas, verificando que ninguno de ellos es, o forma parte de, un virus conocido, con especial atención en los programas ejecutables. Esto puede conseguirse instalando en los puntos de entrada (gateways) de la red y los sistemas filtros que seleccionen y supriman la transmisión de cualquier activo o código dañino no deseado.

4.6 Gestión de la Autoridad de Sistema

Autoridad de Sistema es la concedida a un usuario por asignación de atributos, privilegios o derechos de acceso que están asociados con la operativa del sistema y que son necesarios para realizar actividades de soporte, mantenimiento y operación del propio sistema. Es conocido que los usuarios con este tipo de autoridad pueden usarla, de manera no apropiada, para evitar los controles de Seguridad del sistema y obtener algún beneficio. Esta situación tiene que ser considerada como un abuso de autoridad y sancionada.

1. Los accesos a los Activos de Información del Sistema, que no sean accesibles por un usuario general, tienen que estar basados en una necesidad de acceso válida y vigente, aprobada por el Área de Sistemas. Los usuarios cuyas responsabilidades incluyan el mantenimiento y soporte del sistema, están exentos de tener autorización escrita para acceder a ellos.

2. Los identificadores de usuario definidos para automatizar la operativa pueden ser considerados como parte integrante del sistema y asignados a un Área de soporte y mantenimiento de sistemas, en vez de un individuo. Los usuarios que puedan manejar este tipo de identificadores tienen que tener una necesidad de uso por razones de negocio válida y vigente, aprobada por el Área de Sistemas.

3. Los accesos a los Activos de Información del Sistema pueden ser implantados concediendo el acceso a un grupo de usuarios, siempre que cada acceso de un miembro del grupo pueda ser identificado individualmente. El Área de Sistemas tiene que tener definido e implantado un proceso, incluyendo revisiones periódicas, que asegure la permanente actualización de la lista de acceso y la eliminación de accesos cuando ya no sean necesarios.

4. Las actividades realizadas con Autoridad de Sistema tienen que estar, específicamente, autorizadas por la empresa.

4.7 Gestión de la Autoridad de Administración de Seguridad

Objetivo

Asegurar que sólo los usuarios autorizados pueden añadir, modificar o eliminar funciones de administración de Seguridad del sistema.

Autoridad de Administración de Seguridad es la concedida a un usuario por asignación de atributos o privilegios que están asociados con el Sistema de Control de Acceso y que son necesarios para realizar las actividades de control y administración de seguridad del propio Sistema.

Es conocido que los usuarios con este tipo de privilegios pueden usar, de manera no apropiada, la autoridad concedida para alterar algún componente de Sistema de Control de Accesos que redunde en su beneficio. Esta

situación tiene que ser considerada como un abuso de autoridad y sancionada.

1. La Autoridad de Administración de Seguridad suele ser asignada a usuarios individuales; sin embargo, puede también ser asignada a un usuario automático o a un grupo de usuarios, siempre que se cumplan las siguientes condiciones:

   - Cada acceso de un miembro del grupo pueda ser identificado individualmente.
   - Cada usuario perteneciente al grupo debe cumplir las reglas de este apartado, como si tuviera asignada la autoridad a su usuario individual.

2. Cada asignación a largo plazo (más de un mes) de esta autoridad a un usuario tiene que ser aprobada por escrito por el Área de Sistemas y revalidada cada 12 meses.

3. Cada asignación a corto plazo (hasta un mes) de esta autoridad a un usuario tiene que ser aprobada por el Área de Sistemas, o por un delegado formalmente (por escrito) designado. La aprobación tiene que ser anterior a la asignación de autoridad, aunque en asignaciones por emergencia se puede aprobar con carácter retroactivo.

4. Las actividades realizadas con Autoridad de Administración de Seguridad tienen que estar, específicamente, autorizadas por el Área de Sistemas, por un proceso de control de cambios, o. tienen que ser consistentes con la descripción del puesto de trabajo del usuario que la realiza. La función de Sistemas de Información tiene que asegurarse que los usuarios, que tienen esta autoridad, están informados de ello.

5. Siempre que el Sistema de Control de Accesos lo permita, todas las actividades realizadas con esta autoridad tienen que ser registradas. El registro de estas actividades nunca debe ser desactivado. La función de Sistemas de Información tiene que definir:

- El formato y el contenido de los documentos para la aprobación por escrito de la Autoridad de Administración de Seguridad:
- Un procedimiento para la asignación y aprobación de esta autoridad a corto plazo y en emergencia;
- Un procedimiento para la cancelación de esta autoridad cuando la necesidad de un usuario finaliza;
- Un procedimiento para detectar y corregir cualquier asignación de esta autoridad adquirida sin autorización, incluyendo el bloqueo del usuario que la ha obtenido.

4.8 Registros de Intentos de Acceso

Estos registros podrán ser creados siempre que exista un Sistema de Control de Accesos apropiado. Todos los registros especificados en esta sección, tienen que ser guardados durante, al menos, un año.

Servirán de base para el análisis de cualquier incidente de Seguridad relacionado con los Sistemas de Información y como documentos a revisar en cualquier auditoría.

4.8.1 Registros de acceso al Sistema

Tienen que ser registrados los accesos al sistema y los intentos de acceso inválidos.

4.8.2 Registros de acceso a activos

Tienen que ser registrados los accesos a Activos de Información y los intentos de acceso inválidos.

4.8.3 Registros de actividades

Las actividades realizadas usando la Autoridad de Sistema y la Autoridad de Administración de Seguridad que tienen que ser registradas y su registro nunca pueden ser desactivados.

4.9 Informes de violación de acceso

Objetivo

Asegurar que los intentos de acceso no autorizado, al Sistema o a los activos del sistema, pueden ser reconocidos como una violación, inmediatamente o después del consiguiente análisis.

4.9.1 Accesos Inválidos al Sistema

Tienen que establecerse controles para poder limitar el número de intentos fallidos de conexión al sistema, incluyendo el bloqueo del identificador de usuario, cuando se sobrepase el límite preestablecido por contraseña inválida.

El Área de Sistemas tiene que tener definido e implantado un proceso que le permita obtener informes de los intentos fallidos de acceso al sistema, cuando sean solicitados.

Ataques sistemáticos

El Área de Sistemas tiene que tener definido e implantado un proceso o controles que le permitan detectar, gestionar e informar cuando se produzca un excesivo número de intentos de acceso inválidos al sistema o bloqueo sistemático de usuarios. Para evitar estimaciones subjetivas, cada sistema debe tener previamente fijado un límite a partir del cual se considera que está siendo atacado de forma sistemática.

CAPÍTULO V
DESARROLLO GENERAL DEL PROYECTO

5.1. Protección física

Evitar riesgos potenciales de ataque, pérdida, robo o daño a los Sistemas de Información de la empresa, accidentales o intencionados, que puedan ocasionar la interrupción, total o parcial, de las actividades de negocio. En este capítulo, se pretende definir los medios a utilizar para la protección de las instalaciones donde están situados los recursos informáticos, incluyendo cualquier tipo de soporte físico, que contienen los Activos de Información de la empresa. También se hará referencia a aspectos no directamente relacionados con la Seguridad Informática (relativos a la seguridad de las personas o de las cosas), pero solo con el objeto de tenerlos en cuenta a la hora de planificar una instalación.

5.1.1 Características

Los edificios o instalaciones de la empresa donde estén, o vayan a estar, situados sus Sistemas de Información requieren unas características adicionales de protección física que deben ser consideradas antes de seleccionar su ubicación, teniendo en cuenta:

.

- Estas instalaciones deben estar diseñadas de forma que no se faciliten indicaciones de su propósito ni se pueda identificar la localización de los recursos informáticos.

- Deben incluir zonas destinadas a carga y descarga de suministros, y su inspección de seguridad. Si todos los materiales no pueden ser inspeccionados en el momento, debe habilitarse una zona de consigna o depósito de materiales transeúntes hasta que puedan ser revisados.

- Tienen que disponer de canalizaciones adecuadas para la conducción del cableado de comunicaciones y electricidad, para evitar ataques (sabotaje, fuego, roedores), interceptación o perturbaciones por fuentes de emisión próximas (radio, eléctricas, calor, etc.).

5.1.2 Distribución de las áreas

El edificio o instalaciones de la empresa están distribuidos en varias áreas o zonas que, dependiendo de su utilización y los bienes contenidos, tienen que estar sometidas a una serie de controles de acceso, las instalaciones de acuerdo con los criterios y denominaciones siguientes:

1. **Áreas públicas.** Espacios en los que no hay ningún tipo de restricción de acceso a empleados o personas ajenas a la empresa.

2. **Áreas internas.** Espacios reservados habitualmente a los empleados y personas ajenas a la empresa con autorización por motivos de negocio. Puede haber en ellos recursos informáticos, con un valor bajo.

3. **Áreas de acceso limitado.** Espacios cuyo acceso está reservado a un grupo reducido de empleados, y personas ajenas a la empresa autorizadas por un acuerdo escrito. Pueden concentrarse en ellos recursos informáticos que, en conjunto, tienen un valor medio.

4. **Áreas de acceso restringido.** Espacios cuyo acceso está reservado a un grupo muy reducido de empleados y personas ajenas a la empresa autorizadas por un acuerdo escrito, que tengan necesidad de acceder por razones de negocio. En ellos se concentran Recursos Informáticos que, en conjunto tienen un alto valor o contienen Activos de información críticos para las actividades de negocio.

A las dos últimas (3 y 4) se les denomina Áreas Controladas. Tienen que permanecer cerradas, incluso cuando estén atendidas, y sus accesos controlados.

En las Área controladas, todos los empleados, y las personas ajenas a la empresa con autorización para acceder por razones de negocio, tienen que llevar, permanentemente, y en lugar visible un identificador:

- Los empleados, al menos, con fotografía y nombre (Legible a corta distancia).

- Las restantes personas, al menos, el nombre (legible) y distintivo de la función que cumplen (Ej.: visita, contratado, suministrador, etc.).

Los identificadores de los empleados con acceso a Áreas controladas de cualquier tipo, pueden tener la posibilidad de lectura por banda magnética o por cualquier otro medio, para facilitar el control de accesos y su registro.

Todo identificador, especialmente los que permitan el acceso a Áreas controladas, es personal y debe ser considerado como una contraseña de

acceso físico y no compartirlo con nadie, para evitar estar envuelto en algún incidente de Seguridad no deseado.

Los suministros informáticos que sean peligrosos o combustibles tienen que ser almacenados a una distancia prudencial, no trasladarlos al área donde se encuentran los recursos informáticos hasta el momento de su utilización y retirarlos de la zona inmediatamente después de finalizar su uso.

En las Áreas controladas tiene que estar prohibido: comer, fumar y el consumo de bebidas alcohólicas o cualquier tipo de drogas. Las dos últimas están consideradas de alto riesgo potencial para la instalación, por lo que adicionalmente, debe impedirse la entrada a cualquier Área controlada a las personas de quien se sospeche el consumo, al margen de las acciones de tipo sancionador que hubiera que tomar.

5.1.3 Valoración de las áreas

Los requisitos de control de acceso físico deben basarse en el valor de los Sistemas de Información contenidos en cada Área Controlada y en la importancia que las actividades de negocio suministradas por ellos.

El valor de un Sistema de Información puede obtenerse de acuerdo con los criterios siguientes:

- Alto valor: sistemas corporativos grandes y medios.
- Valor medio: pequeños sistemas corporativos y redes de área local
- Bajo valor: pequeños sistemas (PC) y terminales.

Aunque, para cada caso, deben considerarse otros aspectos tales como:

- El coste y la necesidad de sustitución de los equipos acumulados en un área, o el impacto que podría ocasionar en la empresa la carencia prolongada de una actividad y la no disponibilidad de la información que suministra.

Esto lleva a definir como Sistemas esenciales aquellos que contengan actividades críticas para el negocio de la empresa.

La valoración final debe ser realizada teniendo en cuenta todos los aspectos descritos para definir los requisitos de control de acceso y seleccionar el tipo de Área controlada. Para demostrar la correcta implantación y la efectividad del control de acceso físico, los Administradores de las Áreas Controladas tienen que mantener actualizada, al menos, la documentación siguiente:

- La identificación del área, el uso a que se destina, el nivel de información clasificada soportada, el valor de los equipos, la valoración del servicio y los requisitos de control requeridos.
- La forma de comunicar a los usuarios de los servicios localizados en el área: el nivel de información clasificada soportada, las medidas de seguridad adoptadas y los requisitos para su cumplimiento.

La valoración final, junto con todos los aspectos tenidos en cuenta para ello, tiene que ser documentada y guardada por el Administrador del Área Controlada como documentos auditables.

5.1.4 Medios de protección

5.1.4.1 Sistemas de control

Los responsables del Área controlada tienen que mantener unos controles de acceso efectivos, en proporción a los recursos humanos y el valor de los activos a proteger, que pueden cumplirse de muy diversas formas (ej.: llaves, cierres con clave, sistema electrónico de control de accesos, guardas de seguridad, etc.), pero cualquiera que sea la forma elegida, tiene que cumplir con unos requisitos de auditabilidad mínimos. Los objetivos son:

- Permitir el acceso únicamente a las personas autorizadas por el Administrador del área.
- Registrar (quién, por dónde y cuándo) las entradas y/o salidas.

Para facilitar el control de los accesos a estas áreas, es recomendable la existencia de un único punto o puerta de acceso.

5.1.4.2 Sistemas de detección

Las Área controladas deben contar con medios de detección de situaciones anómalas y previsibles para el área, tales como: puertas abiertas, acceso de intrusos, inundación, incendio o humos, etc.

El objetivo es permitir un conocimiento inmediato y preciso del hecho y su localización, por lo que su actuación debe ser absolutamente fiable dentro de unos parámetros previamente establecidos. Ello exige unas revisiones de funcionamiento y un riguroso mantenimiento preventivo cuya periodicidad dependerá del sistema de detección y del tipo de área controlada al que se aplique.

La detección de un hecho anómalo requiere la información necesaria para una reacción proporcionada. Dependiendo de la información suministrada por el medio de detección y de los parámetros previamente establecidos, antes de llegar a un estado de alarma se puede pasar por un estado de alerta, en el que algunos medios de reacción se van armando en previsión de su posible actuación.

Todos los medios de detección pueden integrarse en un único sistema, preferentemente automático, que los gestione y que:

- Avise de la anomalía y su gravedad;
- Inicie acciones de corrección automáticas

- Proponga acciones manuales a realizar por personal entrenado para ello;
- Controle las actuaciones (qué, quién, cómo, dónde y cuándo).

Este sistema debe estar bajo vigilancia permanente y combinado con los servicios de mantenimiento, para los casos de mal funcionamiento de cualquier medio de detección.

Hay que subrayar que los sistemas de Detección deben funcionar incluso con el suministro eléctrico de emergencia.

5.1.5 Suministros auxiliares

Es esencial la protección de las zonas que albergan los suministros auxiliares que dan servicio a los Sistemas de Información.

Sin una protección, equivalente a los Sistemas que soportan, serían mucho más sencillos de atacar y su destrucción o deterioro acarrearía graves interrupciones del servicio informático. Por tanto, deben estar ubicadas en un área de Acceso Limitado o Restringido, con los controles ya descritos para cada una de ellas.

5.1.5.1 Energía eléctrica

Los Recursos informáticos son sensibles a las variaciones de tensión y de frecuencia de la corriente eléctrica. Los requerimientos básicos para el suministro de energía eléctrica son dos: Calidad y Continuidad.

Relacionado con la calidad, se puede destacar que:

- Las variaciones de frecuencia deben corregirse con equipos estabilizadores que la mantengan dentro de los rangos establecidos por los fabricantes de los Recursos informáticos a alimentar, aunque

algunos Recursos Informáticos de nueva tecnología los llevan incluidos.

- Las variaciones de tensión deben ser manejadas por un Sistema de Alimentación Ininterrumpida (SAI, en inglés UPS), de modo que se puedan prevenir los efectos de posibles microcortes. En relación con la continuidad del suministro eléctrico debe tenerse en cuenta que:

  - Las caídas de tensión pueden ser manejadas por un SAI (UPS), pero solo por tiempo limitado (ya que el desgaste de sus acumuladores es muy rápido y su recarga muy lenta para utilizarlo en cortes sucesivos) y nunca como única alternativa. Las soluciones habituales se basan en una de las siguientes, o en la combinación de varias de ellas:

  - Conexión conmutada a dos compañías suministradoras; o conexión conmutada a dos estaciones transformadoras de la misma compañía, pero situadas en rutas de suministro diferente.

  - Capacidad de transformación de corriente asegurada mediante equipos redundantes; equipos electrógenos, de combustión. Siempre que el volumen de las instalaciones informáticas así lo aconseje.

  - El suministro eléctrico debe ser independiente del general del edificio, y las tomas de tierra deben ser independientes de las generales del edificio, a suficiente distancia de ellas, correctamente instaladas y rigurosamente mantenidas.

Con la evolución tecnológica de los fabricantes, existen en el mercado Recursos Informáticos que reducen (prácticamente eliminan) los tradicionales requerimientos de aire acondicionado.

Sin embargo, debido al parque informático existente y a su antigüedad media, se debe tener en cuenta las siguientes consideraciones:

- Los recursos informáticos, especialmente, los de las grandes instalaciones, generan calor que se hace necesario disipar a través de acondicionamiento de aire, que se encargan de mantener el ambiente con la temperatura y la humedad adecuadas, dentro de los límites indicados por los fabricantes.

- La suficiente potencia y redundancia de estos equipos permitirá que trabajen desahogadamente y que las operaciones de mantenimiento sean sencillas y frecuentes.

- Un elemento fundamental del sistema acondicionador de aire es el mecanismo de corte automático tras producirse una detección de incendio.

5.1.6 Emergencia y Evacuación

Tiene que haber implantado, de acuerdo con las Leyes y reglamentos en vigor, un Plan de emergencia y evacuación de las instalaciones de la empresa.

Los objetivos de este Plan deben ser o conocer los edificios y sus instalaciones, las áreas de posibles riesgos y los medios de protección disponibles:

- Evitar, o al menos minimizar, las causas de las emergencias.
- Garantizar la fiabilidad de los medios de protección.
- Tener informados de las medidas de protección a todos los ocupantes de las instalaciones.
- Disponer de personal organizado y adiestrado para las situaciones de emergencia.
- Hacer cumplir la vigente normativa de seguridad.

Hay que subrayar que la responsabilidad de confeccionar y mantener actualizado el Plan, recae en una función ajena a Sistemas de información. No obstante, es necesaria su colaboración en el desarrollo de las medidas a tomar, relacionadas con las instalaciones informáticas, sus operaciones y las personas que trabajen en ellas.

5.1.7 Impresoras

El término impresora se refiere a cualquier medio o dispositivo que pueda generar salidas impresas.

Se consideran dos tipos de impresoras, según sea su ubicación: las impresoras locales del Sistema, situadas en las áreas de Acceso Limitado/Restringido del propio Sistema y las impresoras remotas que no están situadas en las áreas dedicadas a los sistemas.

- La responsabilidad de especificar las reglas de utilización de cada impresora es del propietario o responsable de ella.
- El control de las salidas impresas es responsabilidad del usuario final que las envía a las impresoras.
- El propietario del sistema o servicio no es responsable de que el propietario o el usuario de las impresoras remotas cumplan con los requerimientos de seguridad descritos en este apartado.

Las salidas impresas de información clasificada tienen que ser protegidas contra accesos no autorizados.

1. Las impresoras remotas situadas en áreas Internas (NO situadas en AAL o AAR), tienen que tener alguno de los controles siguientes:

- Tener designado un responsable de entregar las salidas impresas al usuario final que las envió.
- Estar directamente atendida por el usuario final.
- Recoger los listados personalmente, e inmediatamente después de terminar la impresión.
- Tener la posibilidad de borrado de listados pendientes de impresión.

2. Las impresoras locales o remotas situadas en AAL o AAR, no requieren ningún control adicional para imprimir información clasificada.

5.2 Conexiones externas

Mantener los niveles de protección de los Sistemas de Información cuando, de forma autorizada, sean accedidos por usuarios ajenos a la empresa o por empleados en conexión desde terminales no controlados por la empresa.

Las facilidades que la informática y las comunicaciones ofrecen a los usuarios, permiten ampliar cada vez más el campo de acción y la obtención de información conectándose a redes externas públicas que ofrecen servicios de proceso, red e información.

Al mismo tiempo, las empresas van estableciendo acuerdos de colaboración que implican la autorización de acceso y utilización de Recursos informáticos y Activos de información, bajo determinadas condiciones y en los que la conexión telemática es imprescindible.

Por todo lo anterior, se deduce que, al utilizar una red de comunicaciones externa y no controlada por la empresa, se están utilizando facilidades que pueden representar un riesgo para los Sistemas de Información de la empresa.

A continuación, se incluye la descripción de algunos conceptos que van a ser usados en este capítulo, y al final del mismo un glosario de términos que puede ser de utilidad para su mejor comprensión.

Conexión externa es:

- Un acceso remoto a los Sistemas y Activos de Información internos, por empleados o por terceros, desde terminales que no están controlados por la empresa.
- Un acceso remoto a Sistemas o Activos de Información externos, por empleados, desde terminales controlados por la empresa.
- Una conexión entre un servicio interno y un servicio ajeno a la empresa.

El responsable que define la necesidad de establecer cualquiera de estos tipos de conexión, debe ser considerado como el Administrador de la Conexión.

Controlado por la empresa

Se dice del Recurso informático, generalmente un terminal, que va a ser utilizado para establecer la conexión y que:

- Está en un edificio de la empresa, con los requisitos de control de acceso físico ya descritos
- Está bajó el control directo de la dirección de la empresa, y
- Es usado para el desarrollo del negocio de la empresa.

Gateway

Es el entorno de proceso que permite la conexión, ya sea un recurso informático (hardware), o un Activo de Información (software).

Normalmente, un 'gateway' suministra el enlace de comunicaciones inicial entre Sistemas internos y externos. El Administrador del Sistema que suministra el servicio para el establecimiento de la conexión, debe ser considerado como Administrador del 'gateway'.

Enlace de comunicaciones

Es cualquier medio o tecnología que dé capacidad de teleproceso electrónico. Generalmente, una conexión física.

5.2.1 Responsabilidades del Administrador de la Conexión

El administrador de una conexión externa es responsable de aprobar o denegar su establecimiento, de acuerdo con el informe del equipo revisor, y eliminar cualquier conexión cuando deje de ser necesaria para el negocio de la empresa o expire el plazo de tiempo para el que fue establecida. Adicionalmente, tiene que:

- Utilizar un 'gateway' existente que satisfaga las necesidades de la conexión requerida y cumplir con los procedimientos de autorización de acceso y revalidación periódica de uso existentes.

- Solicitar la creación de un nuevo 'gateway', si ninguno de los existentes satisface las necesidades de la conexión requerida y asegurar que el administrador del 'gateway' recibe e incluye los procedimientos de autorización de acceso y revalidación periódica de uso.

Los procedimientos para autorizar el acceso de usuarios ajenos a la empresa tienen que incluir la verificación de la vigente necesidad por razones de negocio y la revalidación de la autorización de acceso, al menos anualmente.

5.2.2 Del administrador del 'Gateway'

El administrador de un 'gateway' es responsable de:

- Implantar y mantener los controles de seguridad del 'gateway'.
- Verificar los controles de acuerdo con lo descrito en el apartado de certificación de la conexión.
- Aprobar la activación del 'gateway', después de asegurar el cumplimiento de los controles de seguridad.
- Mantener actualizada la relación de usuarios y accesos aprobados para cada 'gateway'.

5.2.3 Del usuario

Todo usuario, ya sea empleado o ajeno a la empresa, que utilice una conexión externa para:

- Acceder a sistemas o servicios ajenos a la empresa, desde un terminal controlado por ella, tiene que cumplir con las normas específicas para este tipo de conexión, con los controles implantados y con cualquier otro procedimiento en uso aplicable al 'gateway' que se esté utilizando.
- Un usuario no puede conectarse simultáneamente a la red interna de la empresa y a otra red externa (no de la empresa). Esta conexión simultánea solo puede ser utilizada, excepcionalmente, por razones

de negocio y con la previa aprobación del Área de Sistemas, para evitar que personas ajenas a la empresa puedan acceder a la red interna a través del terminal del usuario.

Un usuario para conectarse a la red interna desde locales NO controlados por la empresa o a una red externa desde locales controlados por la empresa, tiene que:

- Tener la aprobación previa del Área de Sistemas.

- Conectarse por un 'gateway' seguro, aprobado por el Área de Sistemas; o estar registrado en una Conexión Externa aprobada por la empresa; o ser revalidada su participación, al menos anualmente.

5.2.4 Certificación de la conexión

En una conexión externa, la revisión de certificación es una forma generalmente aceptada, de verificar el cumplimiento de las normas y procedimientos de seguridad implantados en la empresa.

5.2.4.1 Revisión inicial

La revisión inicial y el subsiguiente informe de certificación de seguridad, tiene que ser previa al establecimiento de la conexión.

Tienen que documentarse los procedimientos, resultados e incumplimientos de la revisión inicial, debiendo ser guardados por el Administrador de la conexión externa mientras ésta persista. Si la implantación de las medidas de seguridad resultan inadecuadas o los controles no han sido aplicados correctamente, la conexión no puede ser activada hasta que, en posteriores revisiones, se alcance un total cumplimiento de los requerimientos de seguridad exigidos.

Esta revisión termina con la certificación inicial de Seguridad y el establecimiento de la conexión externa.

5.2.4.2 Revisión anual de recertificación

Tiene que realizarse, al menos, anualmente una revisión de recertificación de características similares a la inicial.

El informe resultante y la documentación relativa a estas revisiones tienen que ser guardados por el Administrador durante toda la vida de la conexión, junto a la de la revisión inicial.

Esta revisión termina con la recertificación de Seguridad y el mantenimiento de la conexión externa.

5.2.4.3 Suspensión de la Conexión

Después de la certificación inicial o de cualquiera de las anuales, pueden producirse cambios que afecten a la integridad de los controles. Tiene que establecerse un proceso para identificarlos e iniciar las pruebas de integridad adecuadas.

Cualquier riesgo detectado durante la vida de la conexión o en las revisiones periódicas tiene que ser identificado, documentado y valorado. Esta valoración tendrá como consecuencia un plan de acción para evitar o minimizar los riesgos. Siempre que los riesgos no puedan ser resueltos inmediatamente, tiene que considerarse la posible Suspensión temporal de la conexión externa, que solo puede ser reactivada a través de un proceso de recertificación.

Tiene que establecerse un proceso para la Suspensión definitiva de una conexión externa, cuando deja de ser

necesaria o expira el plazo para el que fue establecida. Este proceso debe contener la inactivación de todos los usuarios incluidos en ella.

5.2.4.4 El Equipo revisor

El equipo que certifica, tiene que estar compuesto por empleados, o asesores externos, con conocimientos técnicos del entorno y del proceso, pero pueden estar directamente relacionados con la conexión propuesta.

Su misión es intentar penetrar en el sistema o servicio, simulando el acceso de un usuario a través de la conexión externa.

El proceso de revisión, consiste en probar la efectividad de los procedimientos y controles utilizados para cumplir con los requisitos de Seguridad definidos. Para ello, pueden usarse técnicas tales como la inspección del diseño, el código fuente o los datos, los planes de prueba y sus resultados, y cualquier otra técnica que intente forzar los controles de Seguridad implantados, sin interrumpir el normal funcionamiento de los sistemas o servicios.

El equipo revisor tiene que emitir un informe, con la certificación positiva de la conexión o las deficiencias encontradas y las acciones a tomar para ser resueltas.

5.3 Autorizaciones de acceso

La autorización de acceso tiene que ser verificada mediante un identificador de usuario y contraseñas válidas, u otra identificación técnica que cumpla con las normas de seguridad definidas por la empresa.

Una vez verificada la identidad del usuario que está accediendo, no debe haber restricciones para establecer la conexión, salvo las propias de la sesión o servicio con el que vaya a trabajar.

Tiene que haber definidos y establecidos controles para detectar y manejar los ataques sistemáticos contra el ´gateway'.

Conexiones DESDE el exterior

Cualquier acceso, por razones de negocio de la empresa, a los sistemas o servicios internos a través de un 'gateway', tiene que ser justificado por el usuario y registrado en la relación de autorizaciones del 'gateway', a través del cual se vaya a acceder. Todo ello, antes de ser establecida la conexión.

La utilización de esta modalidad, cada vez más frecuente, facilita a un usuario trabajar desde un terminal portátil o desde su propio domicilio.

Conexiones HACIA el exterior

Un 'gateway' puede también ser usado para el acceso a sistemas o servicios ajenos a la empresa, desde terminales controlados por ella. Este tipo de conexión tiene que ser aprobada por el Área de Sistemas antes de ser puesta en funcionamiento y el usuario registrado en la relación de autorizaciones del 'gateway' a través del cual se conecte al exterior.

La utilización de esta modalidad facilita a un usuario la utilización, desde su puesto de trabajo, de redes, sistemas y servicios ajenos a la empresa, pero cada vez más necesarios

Interconexión de redes y sistemas

En el caso de interconexión de redes, sistemas o aplicaciones, la identidad tiene que ser verificada en el momento de la conexión.

5.4 Riesgo a redes inseguras

Cualquier usuario al conectarse con una red que sea, o se presuma que pueda ser, insegura para su simple uso o para comunicarse con organizaciones ajenas a la empresa, tiene que tener en cuenta que puede ser usada por usuarios ajenos a la empresa, en algunos casos de todo el mundo, y por tanto, la información transmitida podrá ser leída, y posteriormente divulgada sin autorización, por muchos desconocidos y no todos desearán el beneficio de la empresa.

5.4.1 Riesgos en redes inseguras

No todos los usuarios utilizan estas conexiones para los fines previstos. Por ello, cualquier acceso desde o hacia una red externa puede representar un riesgo significativo para los activos de información de la empresa, debido a la posible:

- Pérdida de integridad, por corrupción, de Activos de Información, como consecuencia del acceso no autorizado de usuarios a través de un punto de conexión a la red externa sin los controles adecuados.

- Interceptación de información clasificada mientras transita por la red externa. pudiendo ser modificada o robada sin ser detectada por el emisor o el receptor.

- Contaminación por virus, como consecuencia de la obtención de productos infectados procedentes de la red externa.

La protección contra estos riesgos exige una combinación de medidas de protección basadas en normas y procedimientos que los prevengan y en controles que los detecten y eviten (ej.: un Sistema Firewall).

5.4.2 Medidas de protección

Al conectarse a cualquiera de estas redes inseguras desde un terminal controlado por la empresa un usuario tiene que cumplir con unas elementales normas de ética y con las normas de Seguridad definidas por la empresa, entre las que cabe destacar las siguientes: o utilizar los servicios a los que haya sido autorizado.

- Utilizar siempre su propia identidad, nunca una ajena.

- No enviar ni almacenar información clasificada, a menos que esté cifrada.

- No introducir ningún producto sin haber verificado previamente que cumple los requisitos legales de licencia y autorización del fabricante, no obtener ningún producto para usarlo en la empresa, sin previa autorización, debiendo cumplir los requisitos legales de licencia y autorización del fabricante.

- Cualquier producto obtenido en redes externas no puede ser incorporado a los Sistemas de la empresa sin verificar previamente que no contiene ningún tipo de código dañino (virus).

- Si existe un sistema de correo electrónico en la empresa, no usar este tipo de redes como correo interno entre empleados. Los usuarios no deben intentar comprobar la seguridad de la red interna, ni de ninguna red externa.

Las pruebas de integridad de la red están reservadas a una función específica designada por la empresa

5.4.3 Sistema Firewall

Un Sistema Firewall consta de un conjunto de mecanismos, filtros de protocolo y dispositivos de control de accesos que manejan de forma segura la conexión entre una red protegida y una red insegura, tales como Internet o cualquier otra, incluyendo posibles sub-redes inseguras de la propia red interna de la empresa.

Este sistema protege las comunicaciones entre un usuario y una red externa, de la forma más transparente posible para el usuario, facilitándole al máximo los servicios que dicha red ofrece. La mayoría de los sistemas firewall están diseñados para asegurar el tráfico con la red Internet, debido a que representa la mayor fuente de información y de medios de comunicación con terceros, incluyendo: clientes, suministradores y cualquier otro tipo de personas que comparten intereses comunes.

Las fuentes de información se manejan a través del WWW (World Wide Web), que consiste en servidores WEB que contienen información, la mayor parte de uso público, y que son manejados por diversas organizaciones (suministradores, competidores, editores de normas, universidades, etc.).

Un Sistema Firewall está compuesto por:

- Un Sistema de Filtro de Paquetes (Packet Filter System) y
- Un Sistema de Servicios (Services System).

Sistema de filtro de paquetes

Constituye el frente primario entre la red propia y la red externa. Examina todos los paquetes de información intercambiados entre las dos redes y

actúa según el tipo de paquete y las reglas configuradas por el administrador del sistema firewall.

Incluye una zona aislada de la red, llamada Zona Desmilitarizada (ZDM), que contiene información específicamente diseñada para ser compartida por usuarios de redes externas y es usada por:

- Servidores WEB externos,
- Servidores de FTP anónimo y
- Cualquier otro servidor que contenga información pública.

Los servicios de la propia red interna no pueden ser visibles a usuarios de redes externas, en cambio, los servicios que se facilitan al exterior (peticiones de información) son manejados por un servidor conectado a la zona aislada (ZDM).

Los paquetes que contienen direcciones IP desconocidas son rechazados.

Sistema de servicios

El sistema de servicios procesa:

- El correo electrónico (MAIL).
- Las noticias (NEWS).
- Las peticiones de transferencia de Activos (FTP)
- Las peticiones de Telnet (conexión a un servidor Internet).

Todo ello es manejado por un servidor, de autenticación antes de que sea permitido el proceso.

Las direcciones IP de la red interna tienen que cambiarse a direcciones IP del Firewall, antes de su salida al exterior, de forma que no sean visibles en

el tráfico originado por el Firewall. Ocultar datos sobre la estructura interna (direcciones IP, identificaciones de nodos, etc.) ayuda a prevenir ataques del exterior.

5.4.4 Transferencia de activos

La transmisión de mensajes, notas y documentos o datos y programas se considera una transferencia de Activos, siempre que se realice a través de un 'gateway' y desde o hacia un servicio interno de la empresa.

Tiene que haber un proceso que asegure la notificación de transmisiones no autorizadas al propietario del 'gateway' y poderlas prevenir y/o interrumpir. Debe considerarse NO autorizada la transmisión de material ofensivo o amoral y los Activos que contengan virus, y adicionalmente el uso con fines fraudulentos de la red interna de la empresa.

5.4.4.1 Correo electrónico

Es un medio de comunicación entre empleados, generalmente dentro del ámbito de la empresa, aunque también fuera de ella, que va adquiriendo un uso creciente. Este medio concebido para la transmisión de mensajes o notas, permite habitualmente la transmisión de todo tipo de Activos.

Además de las consideraciones generales de Seguridad, hay que tener en cuenta:

- La posibilidad de interceptación de mensajes o notas, por lo que no debe incluirse en ellos información sensible que no esté cifrada.
- La posible inclusión de virus o código dañino en los activos de información recibidos.

5.4.4.2 EDI (Electronic Data Interchange)

Es un estándar ISO para el Intercambio Electrónico de Datos en formato normalizado, entre los Sistemas de Información (y sus nodos de comunicaciones) de los participantes en transacciones comerciales.

Tiene que haber un acuerdo contractual, entre los participantes en el intercambio, sobre los derechos y deberes en la cesión y adquisición de información, así como los requisitos documentales y de prueba a ser utilizados en caso de litigio. El contrato debe contener aspectos tales como:

- Procedimientos a utilizar para las transacciones; o medios técnicos que intervendrán;
- Criterios de aceptación o rechazo de los documentos electrónicos;
- Responsabilidades del emisor de la Información;
- Responsabilidades del receptor de la Información.

CONCLUSIONES

1. Los incidentes de seguridad impactan en forma cada vez más directa en la empresa, en consecuencia, se requieren efectivas acciones de concientización, capacitación y mantener un estado de alerta y actualización permanente.

2. Debido a las cambiantes condiciones y nuevas plataformas de computación disponibles, es vital el desarrollo de documentos y directrices que orienten a los empleados en el uso adecuado de las tecnologías.

3. Solo el personal autorizado tienen los permisos para acceder a la información de la empresa, para proteger la información contra accesos no autorizados.

RECOMENDACIONES

1. No instalar software del cual desconozca su procedencia; para cualquier instalación solicitar el apoyo técnico del Área de Sistemas, que le brindará la asesoría correspondiente.

2. No descargue ni mantenga archivos de música o vídeos en los equipos asignados.

3. Asegúrese de que su equipo asignado tenga el antivirus y controles de seguridad activos.

4. Absténgase de descargar archivos adjuntos de correos electrónicos con mensajes sugestivos.

5. En los perfiles de las redes sociales no de mayor información, puede ser usada por personas inescrupulosas.

6. Sea muy cuidadoso con los dispositivos como USB o discos externos estos son bastante susceptibles a infecciones de virus informáticos, cambie frecuentemente sus claves de acceso a los sistemas.

FUENTES DE INFORMACIÓN

Bibliográficas:

1. Fish, G.B. (20100). "*Secure Computers and Networks*". Estados Unidos. White Press.

2. Morant, S. (2011). "*Seguridad de la Información*". México. Centro de Ramón Areces.

3. Stollings (2012). "*Network and Internet Netwok Security*". Canadá. Prentice Hall.

4. Northcutt, L.; Zellses, S.; Winter (2012). "*Inside Network Perimeter Security. The Definitive Guide of Firewalls Virtual Private Networks Router and Intrusion Detection System*". Inglaterra. Editorial Sams.

.

ANEXOS

1. Glosario de términos
2. Cronograma del proyecto

ANEXO 1

GLOSARIO DE TÉRMINOS

Adware:

Aplicaciones que durante su funcionamiento despliegan publicidad en ventanas emergentes o barras de herramientas a cambio de la gratuidad en su utilización. La publicidad normalmente permite visitar la página web del anunciante, por lo que requiere conexión a internet para funcionar. Se diferencian de los programas gratuitos (*Freeware*) en que incorporan publicidad. La mayoría de los programas publicitarios son confiables, pero en ocasiones algunos de ellos son utilizados con fines poco éticos llegando a comportarse como auténticos programas espías. Sirviendo a las empresas patrocinadoras de los mismos para controlar movimientos de los usuarios.

AdWords:

Sistema de Google de anuncios publicitarios de texto o gráficos, que usualmente aparecen en el lado derecho de la pantalla de los resultados de búsqueda. También pueden aparecer en la red de sitios web que están afiliados a AdSense de Google.

AdSense:

Es un sistema de publicidad online propiedad de Google. Los dueños de los sitios web pueden incorporarse al programa AdSense para generar dinero por la publicidad que miran sus visitantes. Los Webmasters afiliados a Adsense ganan por cada clic que sus visitantes hacen en la publicidad .

Agujero de Seguridad :

Es una vulnerabilidad, es un error en una aplicación o sistema operativo por el cual se compromete de alguna manera la seguridad del equipo donde se está ejecutando dicho programa vulnerable.

Análisis Heurístico:

Sistema de análisis que tienen algunos antivirus basados en la suposición de comportamientos en vez de contrastar fragmentos de código con patrones previamente conocidos como nocivos. El análisis heurístico aplicado a antivirus busca nuevas especies de virus que se comporten de forma no pre-estudiada en especies anteriormente encontradas, permitiendo así, detectar nuevos virus antes de que se expandan y distribuyan por las redes. Esta mecánica es útil para prevenir infecciones desconocidas, sin embargo, debe usarse con cuidado ya que aumenta las falsas alarmas de los antivirus o los falsos positivos detectados. Como usuario, al encontrar un aviso de un archivo infectado con un tipo de virus desconocido o nuevo, debemos reportarlo a la empresa del antivirus para que lo analicen adecuadamente y si realmente es un virus, desarrollen la forma de limpiarlo.

Ancho de Banda:

Bandwidth en inglés. Cantidad de bits que pueden viajar por un medio físico (cable coaxial, par trenzado, fibra óptica, etc.) de forma que

mientras mayor sea el ancho de banda más rápido se obtendrá la información.

Antivirus:

Programa cuya finalidad es prevenir los virus informáticos así como curar los ya existentes en un sistema. Estos programas deben actualizarse periódicamente.

Anti – Rastreo:

Característica de algunos programas maliciosos como los virus y también un conjunto de técnicas utilizadas por los programadores de virus, spammers y gente que se dedica a difundir malware, emplean para evitar ser detectados e investigados. El término en inglés es anti-debug.

Arin:

American Registry of Internet Numbers. Organización en Estados Unidos que gestiona las direcciones IP del país, y sus territorios asignados. Debido a que las direcciones en Internet deben de ser únicas y los espacios de direcciones en Internet son limitados, es necesaria una organización que controle y asigne los bloques numéricos.

Ataque Cibernético:

Ataque contra la infraestructura informática de un país. Es también un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático.

ATM:

Acrónimo en inglés de Asynchronous Transfer Mode. Modo de Transferencia Asincrónica. Es una tecnología de redes de alta velocidad que

transmite múltiples tipos de información (voz, vídeo, datos) mediante la creación de "paquetes de datos".

Autenticación:

Técnica mediante la cual un proceso comprueba que su compañero de comunicación es quien se supone que es y no un impostor.

Back Door Puerta Falsa, Trasera:

Técnica de Hacking que permite introducirse en los programas por puntos que no son los estándares o normales. En principio eran utilizados por los programadores para facilitar el proceso de pruebas, evitando tener que procesar todo el programa o sistema para probar sólo un trozo. Si estas puertas falsas se mantienen en la versión operativa, bien de forma intencionada o por descuido, se crean agujeros en la seguridad de la aplicación.

Biometría:

La biometría es una tecnología basada en el reconocimiento de una característica de seguridad y en una física e intransferible de las personas, como por ejemplo la huella dactilar.

Black Hat:

Hacker que busca en los sistemas informáticos de una manera maliciosa, buscando una satisfacción personal y/o económica. Muestra sus habilidades en informática rompiendo computadoras, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, entre otras muchas cosas utilizando sus destrezas en métodos Hacking.

Bluetooth:

Es un tipo de conexión inalámbrica entre dispositivos que tiene un alcance de varios metros, popularizado por la telefonía móvil. Se usa, por ejemplo, para transferir una foto o un vídeo de un móvil a otro, de forma gratuita. Para hacer eso no es necesario conocer el número de teléfono del receptor: al activar nuestro Bluetooth, el teléfono detecta automáticamente todos los teléfonos a su alcance que también lo tengan activado.

Bridge:

En redes de computadoras, un "bridge" (puente), conecta dos o más redes de área local (LAN).

Browser:

Aplicación para visualizar todo tipo de información y navegar por el www con funcionalidades plenamente multimedia. Como ejemplo de navegadores tenemos Internet Explorer, Firefox, Chrome y Safari.

Browser Hijackers:

Programas que cambian la página de inicio y búsqueda entre otros ajustes del navegador web, se dice que secuestran el navegador. Estos pueden ser instalados en el sistema sin nuestro consentimiento al visitar ciertos sitos web mediante controles ActiveX o bien ser incluidos por un virus troyano.

Bucaneros:

Comerciantes de la red relacionados con hackers y crackers aunque no existen en ella; aunque no poseen ningún tipo de formación en el

área de los sistemas, si poseen un amplio conocimiento en área de los negocios.

Carder:

Es aquella persona que maneja la información y las herramientas necesarias para robar dinero de tarjetas de crédito ajenas.

Carding:

Robo de identidad y uso fraudulento de tarjetas de crédito.

Certificado Digital:

Acreditación emitida por una entidad o un particular debidamente autorizada garantizando que un determinado dato (una firma electrónica o una clave pública) pertenece realmente a quien se supone. Documento digital que garantiza que alguien es realmente quien dice ser. Además de la identificación, los certificados digitales nos permiten firmar y cifrar contenidos.

Certificado Electrónico:

Documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Chain Email:

Es cualquier email enviado a una o más personas pidiéndoles que reenvíen el mensaje a una o más personas, con la promesa de una recompensa por reenviarlo o castigo en caso de no hacerlo.

Cheater:

Personas que hacen trampas en los videojuegos para tener ventaja sobre otros jugadores. Para ello, recurren a debilidades en el código de programación de un título o utilizan software no autorizado.

Cibermarketing:

Se define como las normas y estrategias que se utilizan para vender dentro del comercio electrónico y las redes de internet. Las corrientes de venta con el comercio electrónico, los cambios en la publicidad gracias a Google y Facebook van generando las normas de mercadotecnia que rigen en internet.

Cifrado:

Método que consiste en convertir el contenido de un archivo en código. De este modo nadie puede verlo a menos que tenga la clave. También se pueden cifrar unidades en Windows 7 y Vista.

Codec:

Corto para comprimir/descomprimir, un codec es cualquier tecnología para comprimir y descomprimir data. codecs pueden ser implementados en software, hardware o en la combinación de ambos.

Confidencialidad:

Técnica mediante la cual tanto el emisor como el receptor, pueden estar seguros de que el mensaje no ha podido ser leído por una tercera parte no deseada.

Contraseña Segura:

Contraseña verificada con distintos grados de seguridad con programas. Para que sea segura deberá contener letras, números y símbolos.

Contraseña: Password

Código utilizado para acceder a un sistema restringido. Pueden contener caracteres alfanuméricos e incluso algunos otros símbolos. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

Copyhacker:

Generación de hackers falsificadores dedicados al crackeo de Hardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura y después venderlos los bucaneros.

Cortafuegos: Firewall

Parte del ordenador o de la red que bloque accesos no autorizados y permite comunicaciones consideradas seguras. Programa hardware o software diseñado para impedir que los hackers usen su computadora para enviar información personal sin su autorización. Los programas firewall vigilan los intentos exteriores de acceder a su sistema y bloquean las comunicaciones de y hacia fuentes no autorizadas por el usuario. Programa que controla las entradas y las salidas de datos de nuestro ordenador, de manera que puede evitar que algún experto malintencionado entrase a por nuestros datos.

Crack:

Es un pequeño código que sirve para saltarse las protecciones anticopia de un programa que se ha descargado ilegalmente. Por ejemplo, puede hacer que una versión gratuita de prueba siga funcionando después de la fecha de expiración sin tener que comprarlo, o que no haga falta introducir el código de la licencia (es ilegal utilizar un programa sin licencia). También hay cracks que permiten hacer trampas en los videojuegos.

Cracker:

Derivación de la expresión "criminal hacker". Creado alrededor de 1985 por contraposición al término hacker, en defensa de éstos últimos por el uso incorrecto del término. Se considera que la actividad realizada por esta clase de cracker es dañina e ilegal. Por ello los crackers son criticados por la mayoría de hackers, por el desprestigio que les supone ante la opinión pública y las empresas, son aquellos que utilizan sus conocimientos técnicos para perturbar procesos informáticos. Pueden considerarse un subgrupo marginal de la comunidad de hackers. Persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un Cracker es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos. Persona que trata de introducirse a un sistema sin autorización y con la intención de realizar algún tipo de daño u obtener un beneficio. Persona que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

Crimeware:

Cualquier tipo de malware que ha sido diseñado y desarrollado para perpetrar un crimen del tipo financiero o económico. Originalmente, el crimeware abarcaba dos acciones principales: el robo de credenciales en

línea, es decir, de cualquier dato que pueda ser utilizado para identificar a un usuario; y la realización de transacciones comerciales o financieras no autorizadas, robos, estafas, fraudes o timos financieros llevados a cabo con los datos obtenidos. En la actualidad, sin embargo, esta definición engloba además a todos los procedimientos que sirven de objetivo y plataforma para soportar esas acciones delictivas.

Criptoanálisis:

Es el estudio de los métodos para obtener el sentido de una información cifrada, sin acceso a la información secreta requerida para obtener este sentido normalmente. Típicamente, esto se traduce en conseguir la clave secreta. En el lenguaje no técnico, se conoce esta práctica como romper o forzar el código, aunque esta expresión tiene un significado específico dentro del argot técnico.

Criptografía:

Se dice que cualquier procedimiento es criptográfico si permite a un emisor ocultar el contenido de un mensaje de modo que sólo personas en posesión de determinada clave puedan leerlo, luego de haberlo descifrado.

Criptovirus:

Tipo de malware que "secuestra" archivos del usuario y luego pide un "rescate" en dinero para liberarlos.

Cuarentena:

Función de protección característica de los antivirus que nos permite dejar sin efecto a archivos que puedan estar infectados, hasta que nuestros sistemas de seguridad tengan una nueva actualización para poder

desinfectarlos o hasta que el administrador decida qué hacer con ellos, si desinfectarlos o borrarlos directamente.

Desfragmentar:

Desfragmentar un disco duro es el proceso en el cual se reorganiza la data del disco duro para que este de una manera más eficiente, por lo tanto, el disco duro funciona más rápido y mejor

Dropper:

Es un fichero que al ejecutarse dispersa lentamente un virus. Un fichero “dropper” puede crear un virus e infectar el ordenador al ejecutarse. Cuando un “dropper” es escaneado por un antivirus, generalmente no se detectará un virus, porque el código viral no ha sido creado todavía. El virus se crea en el momento que se ejecuta el “dropper”.

Encriptación:

Tratamiento de un conjunto de datos, contenidos o no en un paquete, a fin de impedir que nadie excepto el destinatario de los mismos pueda leerlos. Hay muchos tipos de cifrado de datos, que constituyen la base de la seguridad de la red.

Encriptar:

Guardar un archivo mediante un programa que lo codifica para que no sea legible ni accesible a menos que se conozca la contraseña que pone el usuario. Se hace para proteger un archivo con contenido confidencial o enviarlo de forma segura a otra persona.

Esteganografía:

Disciplina en la que se estudian y aplican técnicas que permiten el ocultamiento de mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia. Es una mezcla de artes y técnicas que se combinan para conformar la práctica de ocultar y enviar información sensible en un portador que pueda pasar desapercibido.

Filtro Antispam:

Es una aplicación que tienen la mayoría de servicios de correo electrónico, que utiliza complejos algoritmos, que permite identificar y bloquear el correo electrónico no deseado.

Firma Digital:

Información cifrada que identifica al autor de un documento electrónico y autentica su identidad.

Firma Electrónica:

Conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.

Firewall: Cortafuegos

Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios. Los cortafuegos pueden ser implementados en hardware y software o en una combinación de ambos. Se utilizan con frecuencia para evitar que los usuarios de internet no autorizados tengan acceso a redes privadas conectadas a internet, especialmente intranets.

Freenet:

Freenet es un programa gratuito, que te permite publicar y obtener información en el internet sin censura. Para lograrlo, la red Freenet es totalmente descentralizada y todos los usuarios y escritores son anónimos.

Función Hash:

Operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales.

Gateway: Puerta de Enlace

Es el dispositivo que permite interconectar redes de computadoras con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información utilizado en una red inicial, al protocolo usado en la red de destino. La puerta de enlace es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones de red (Network Address Translation, NAT). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada enmascaramiento de IP, usada muy a menudo para dar acceso a Internet a los equipos de una LAN compartiendo una única conexión a Internet y por lo tanto, una única dirección IP externa.

Gusano:

Software malicioso capaz de autorreplicarse y extenderse de un ordenador a otro, que puede llevar código malicioso oculto en su interior que permitiría abrir puertas traseras y convertirlo en un ordenador zombie.

Programa informático que se autoduplica y autopropaga. En contraste con los virus, los gusanos suelen estar especialmente escritos para redes. Los gusanos de redes fueron definidos por primera vez por Shoch & Hupp, de Xerox, en la revista ACM Communications.

Hacker:

Alguien que realiza personalizaciones y combinaciones innovadoras de dispositivos electrónicos o informáticos estándar con el fin de darles usos para los que nos estaban pensados originalmente. Persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de acceder a cualquier tipo de "información segura". Su formación y las habilidades que poseen les da una experiencia mayor que les permite acceder a sistemas de información seguros, sin ser descubiertos, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.

Hacking Etico:

Hacking ético es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

Hacker Semántico:

Técnica que altera la información para que parezca correcta, no siéndolo. Ejemplo: un sistema de temperatura controlado por ordenador

podría mantener valores aparentemente bajos siendo peligrosamente altos. Puede suponer una amenaza para procesos industriales y de infraestructura nacional.

Holograma:

Característica desarrollada para uso exclusivo en documentos de alta seguridad. Es una estructura de difracción microscópica cuya imagen es tridimensional a todo color, diagramadas mediante un proceso especial de rayos láser. Son imágenes tridimensionales a todo color, diagramadas mediante un proceso especial de rayos láser. En papel moneda se emplean otras variantes como el iniciático pixelgrama y los actuales, y más populares, kinegramas.

Intrusión:

Cuando un pirata informático, accede sin autorización al equipo de un usuario de forma que el usuario no se dé cuenta, y ya con el control de esa máquina, puede realizar cualquier tipo de actividades. También se pueden dar intrusiones a redes locales, por ejemplo, la de una empresa, y así obtener información sensible y confidencial.

Internet:

Es un conjunto descentralizado de redes de comunicaciones interconectados que utilizan la familia de protocolos TCP / IP. Uno de los servicios que más éxito ha tenido en Internet ha sido la Word Wide Web. Hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto y utiliza Internet como medio de trasmisión.

IP:

Protocolo de Internet. Conjunto de reglas que regulan la transmisión de paquetes de datos a través de Internet. El IP es la dirección numérica de una computadora en Internet de forma que cada dirección electrónica se asigna a una computadora conectada a Internet y por lo tanto es única. La dirección IP está compuesta de cuatro octetos como por ejemplo, 132.248.53.10

IP spoofing:

Técnica que permite que un bandido tome la identidad de un host "confiable" (cambiando su dirección IP por la dirección de éste) y obtenga de este modo accesos no autorizados a otros sistemas.

Joker:

Programas que tienen como objetivo hacer creer a los usuarios que sus equipos han sido afectados por un virus. Para conseguirlo muestran falsos mensajes que advierten de la inminente realización de acciones destructivas en el ordenador, modificando la configuración de la pantalla.

Keygen:

Se denominan así, a los programas creados por Crackers, los cuales son capaces de generar las claves de registro de un programa shareware. Estos generadores de registro, normalmente muestran el número de serie a introducir en la aplicación que se quiere registrar.

Keyloggers:

Programas que se instalan en el PC y registran actividad, datos personales y tecleados sin que la víctima se dé cuenta y con las que los delincuentes pueden encontrar nombres contraseñas o números de cuenta.

Kinegrama:

Característica desarrollada para uso exclusivo en documentos de alta seguridad. Es una estructura de difracción microscópica cuya imagen no es tridimensional, como en el holograma, sino que al moverla muestra animaciones gráficas. Se presentan en tiras, a modo de hilos de seguridad, o en parches. Jurídicamente el Kinegrama da más solidez y seguridad a un documento legal, básicamente notarial, los cuales ya vienen numerados y sabe perfectamente que Notario emitió el documento y otros datos más generales, como numero de testimonio, acto que se protocoliza y personas que intervienen.

Módulo Criptográfico Hardware de Seguridad:

Módulo hardware utilizado para realizar funciones criptográficas y almacenar claves en modo seguro.

P2P, Peer to peer:

Programas de intercambio de archivos entre usuarios. Cada uno comparte con los demás los datos y archivos que quiera desde su propio ordenador, y al mismo tiempo tiene acceso a todo lo que comparten los demás. La diferencia con descargar algo de Internet es que en el p2p los datos no llegan a subirse nunca a la web se transmiten directamente de un ordenador a otro. Es un modelo de comunicaciones en el cual cada parte tiene las mismas capacidades y cualquiera de ellas puede iniciar la comunicación. Otro modelo totalmente opuesto es el cliente/servidor en donde el servidor se encuentra a la espera de una comunicación por parte del cliente. Este modelo se basa en que ambos nodos actúen como servidores y clientes a la vez.

PAP:

(Password Authentication Protocol) Protocolo de Autentificación por Password. Protocolo que permite al sistema verificar la identidad del otro punto de la conexión mediante una contraseña.

Payload:

Función adicional que posee cierta amenaza en particular. La traducción exacta del inglés, es más precisa respecto a su definición: "carga útil". Refiere a acciones adicionales, incluidas en virus, gusanos o troyanos; como por ejemplo robo de datos, eliminación de archivos, sobre-escritura del disco, reemplazo del BIOS, etc. Un payload no es necesariamente maligno, sino que refiere también a efectos secundarios nocivos para el ordenador.

Pharming:

Se denomina Pharming al acto de explotar una vulnerabilidad en el software de un servidor de DNS, que permite que una persona se "adueñe" del dominio de un website, por ejemplo, y redirija el tráfico hacia otro sitio. Técnica de manipulación de la resolución de nombres y direcciones legítimas producido por un código malicioso, normalmente en forma de troyano, que se introduce en el ordenador mientras se realiza una descarga, a través de spam, copiando desde un CD-Rom, etc., rediccionando a una web ilegítima. Simplificando, el pharming consistiría en que, estando el ordenador infectado por un troyano o programa que permita realizar los cambios en las DNS, accedería a una web introduciendo para ello la URL y se realizarían compras o accesos a cuentas bancarias en una página falsa, con lo que finalmente los atacantes obtendrían códigos secretos y por ende la puerta abierta para cometer el fraude.

Phishing:

Estafa con robo de datos personales principalmente bancarios a través de e-mails engañosos que parecen auténticos (logotipos y direcciones Web) y otras técnicas. Accede a tus cuentas bancarias. SPEAR – PHISHING: Phising captando datos de redes sociales, Blogs y Bitácoras principalmente se refiere a comunicaciones fraudulentas diseñadas para inducir a los consumidores a divulgar información personal, financiera o sobre su cuenta, incluyendo nombre de usuario y contraseña, información sobre tarjetas de crédito, entre otros.

Phreaker:

De phone freak ("monstruo telefónico"). Son personas con conocimientos tanto en teléfonos modulares (TM) como en teléfonos móviles, se encuentran sumergidos en entendimientos de telecomunicaciones bastante amplios. Por lo general trabajan en el mercado negro de celulares, desbloqueando, clonando o programando nuevamente los celulares robados. Hacker o cracker que se caracterizan por poseer vastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los celulares, han tenido que ingresar también al mundo de la informática y del procesamiento de datos. Persona que hackea las redes telefónicas ajenas para evitar pagar llamadas a larga distancia.

Pirata Informático:

Delincuente informático. Este personaje dedicado a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etc., de una manera consciente o inconsciente uno se convierte en un pirata informático descargando programas, juegos, música.

Radius:

Siglas del inglés Remote Authentication Dial In User Service. Permite la administración centralizada de data de autenticación, como por ejemplo usuario y passwords.

Ransomware:

Amenaza informática similar a un ataque sin medios tecnológicos similar al secuestro. Es un código malicioso que cifra la información del ordenador e introduce en él una serie de instrucciones para que el usuario pueda recuperar sus archivos. La víctima, para obtener la contraseña que libera la información, debe pagar al atacante una suma de dinero, según las instrucciones que este disponga. El pago generalmente es indicado a través de un depósito bancario, después del cuál el atacante envía las contraseñas para descifrar la información del disco duro. En las primeras versiones, los métodos de cifrado utilizados fueron de lo más precarios y recuperar la información era una tarea viable sin entregar el dinero al atacante.

Reverse Engineering:

Se denomina al intento de descubrir el diseño a partir de la máquina. No es una actividad ilegal. También se conoce con este término la actividad del 'cracking', en su vertiente de desproteger programas.

Robo de Identidad:

Delito en alza que consiste en el robo de información personal de la víctima para después abrir con ella cuentas bancarias, reclamar beneficios y solicitar tarjetas de crédito o permisos de conducir. Consiste en realizar acciones utilizando los datos de otra persona. Como lo más normal es que esas acciones sean ilegales: compras online con tarjetas robadas, apertura de cuentas bancarias, este tipo de ataques suelen tener graves consecuencias para los usuarios que han sido víctima de ellos. Como norma

general, se define que ha habido un robo de identidad cuando una persona utiliza la información personal de otra, como nombre, dirección, número de Seguro Social, para realizar actividades ilegales como abrir cuentas de crédito, sacar dinero del banco o hacer compras.

Rogue / Rogueware:

FakeAVs, Badware, Scareware. Falso programa de seguridad. Software que, simulando ser una aplicación anti-malware (o de seguridad), realiza justamente los efectos contrarios a estas: instalar malware. Por lo general, son ataques que muestran en la pantalla del usuario advertencias llamativas respecto a la existencia de infecciones en el equipo del usuario. La persona, es invitada a descargar una solución o, en algunos casos, a pagar por ella. Los objetivos, según el caso, varían desde instalar malware adicional en el equipo para obtener información confidencial o, directamente, la obtención de dinero a través del ataque.

Rootkit:

Programa que se oculta y hace que ciertos virus pasen desapercibidos.

Router:

Es un procesador de redes interconectadas que encamina paquetes de datos entre dos, o más, redes conectadas. El router IP encamina datagramas entre redes directamente conectadas o adyacentes.

Samurai:

Persona contratada para investigar fallos de seguridad, que investiga casos de derechos de privacidad, esté amparado por la primera enmienda estadounidense o cualquier otra razón de peso que legitime acciones semejantes. Los samuráis desdeñan a los crackers y a todo tipo de

vándalos electrónicos. También se dedican a hacer y decir cómo saber sobre la seguridad con sistemas en redes. También se dedican a hacer y decir cómo saber sobre la seguridad con sistemas en redes. Sinónimo de amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo.

Scam:

Nombre usado para las estafas a través de medios tecnológicos. Delito consistente en provocar un perjuicio patrimonial a alguien mediante engaño y con ánimo de lucro; utilizando como medio la tecnología. Es una web falsa, sin suplantación de legítimas marcas y que al final recaban datos personales y / o bancarios. Los medios para ello son similares a los que utiliza el phishing; aunque el objetivo no es obtener datos sino lucrar de forma directa a través del engaño. Las técnicas utilizadas principalmente, para engañar al usuario, son el anuncio de una ganancia extraordinaria o las peticiones de ayuda caritativa. En el primer caso aparecen, por ejemplo, los anuncios de empleo con rentabilidades inesperadas o el premio de una lotería o juegos de azar, en los que se le solicita al usuario que haga una entrega de una pequeña suma de dinero (en comparación con la supuesta ganancia ofrecida) para poder verificar algunos datos o cubrir los costos de envío y administración del dinero obtenido. El segundo caso, y el más común, es el correo solicitando una donación al usuario, para una obra caritativa. Los contenidos más generales hacen referencia a países de extrema pobreza (generalmente de África), a personas enfermas o a catástrofes internacionales. El correo invita a la víctima a hacer un depósito o envío de dinero a fin de colaborar con la causa caritativa. Esta técnica de ingeniería social ataca la bondad de las personas y su interés por ayudar. Los scam son una amenaza constante para el usuario y cientos de ellos rondan la red cada día. Sin embargo, después de algún desastre (terremoto, inundación, guerra, hambruna) con algún impacto mediático considerable, aumenta notablemente la cantidad de correos scam que circulan por la red.

Skimmin:

Clonación de tarjetas de crédito o debito, consiste en la duplicación de tarjetas de crédito o debito sin el consentimiento del dueño de la tarjeta. Los delincuentes que se dedican a esto utilizan diferentes tipos de dispositivos electrónicos que los ayudan a clonar de las tarjetas. El problema es que los dueños de las tarjetas de crédito o debito no se dan cuenta de esto hasta que les llega el estado de cuenta o cuando van a comprar algo en una tienda o por internet con su tarjeta y le dicen que su tarjeta está al límite o se la rechazan. Y cuando esto sucede quiere decir que ya le robaron su identidad.

Smishing:

Técnica de estafa similar al Phishing y al Vishing pero a través del teléfono móvil, utilizando un SMS ‘gancho' para robar datos. Consiste en el envío de un mensaje corto SMS a un usuario indicándole que se ha suscrito a un determinado servicio, y que de no cancelar la suscripción mediante un mensaje corto al número indicado. En el mensaje de respuesta, se le pueden demandar ciertos datos personales al usuario. La forma de protegerse del “smishing” es bien sencilla a la vez que obvia. Si usted recibe un mensaje corto que no ha demandado, simplemente bórrelo. Ya sea una solicitud de respuesta, una melodía gratuita o él último logo de moda, lo más sencillo y seguro es que borre el SMS de la memoria de la tarjeta SIM.

Sniffer:

Programa que busca palabras claves que se le hayan impartido en los paquetes que atraviesan un nodo con el objetivo de conseguir información y normalmente se usa para fines ilegales. Programas que se ejecutan en una red informática y rastrean todas las transacciones que viajan por ella para volcarlas en un fichero. El estudio de este fichero permite encontrar claves, passwords o números de tarjetas de crédito, que pueden ser utilizados de forma fraudulenta. En general los programas están escritos

en lenguaje C y pueden encontrarse disponibles en algunos foros de debate de Internet.

Sniffing:

Dispositivos que permiten al atacante “escuchar” las diversas comunicaciones que se establecen entre ordenadores a través de una red (física o inalámbrica) sin necesidad de acceder física ni virtualmente a su ordenador.

Spam:

Correo basura. E-mail o mensajes instantáneos enviados sin consentimiento del destinatario. Pueden incluir virus en archivos adjuntos o enlaces dudosos que convierte el PC en un PC ZOMBIE. Suelen anunciar viagras, extensores y otras estafas. Correo masivo no solicitado que se envía sin saber si el destinatario tiene el mínimo interés en el mensaje. Se genera por comerciantes de pocos escrúpulos y suelen utilizarlo para promocionar productos o servicios ilegales o poco recomendables. El correo electrónico es uno de los sistemas de comunicación más baratos que existen, y por eso los spammers tienen tanto interés en él. Envío masivo, indiscriminado y no solicitado de publicidad a través de email, aunque actualmente las personas se refieren como spam a publicidad que llega a los celulares por medio de mensajes de texto SMS.

Spamboot:

Pequeños programas o robots buscadores de email para infectarlos con Spam.

Spamer:

Individuo que crea y distribuye de forma masiva mensajes de correo electrónico basura, también llamado spam.

Spoofing:

Procedimiento que cambia la fuente de origen de un conjunto de datos en una red, por ejemplo, adoptando otra identidad de remitente con el fin de engañar a un servidor firewall. Técnica que consiste en alterar el aspecto de páginas y mensajes para que parezcan auténticos.

Spyware:

Programa que se instala en el PC sin permiso del usuario y recopila información de la actividad y datos personales. Spyware son unos pequeños programas cuyo objetivo es mandar información, generalmente a empresas de mercadeo, del uso de internet, websites visitados, etc. del usuario, por medio del internet.

Stealer:

Nombre genérico de programas informáticos maliciosos del tipo troyano, que se introducen a través de internet en un ordenador con el propósito de obtener de forma fraudulenta información confidencial del propietario, tal como su nombre de acceso a sitios web, contraseña o número de tarjeta de crédito. Infostealer puede afectar también al servicio de correo electrónico MSN Messenger, enviando mensajes falsos e incluso introduciendo en ellos datos incluidos por los usuarios en sus mensajes a través de dicho servicio. Otro problema causado por stealer puede ser la desconexión involuntaria de un sitio web. Estos programas pueden detectarse y eliminarse mediante software antivirus, aunque la mejor forma de evitarlos consiste en no abrir documentos anexos a correos electrónicos enviados por remitentes desconocidos o dudosos.

TCP / IP:

Protocolo de Control de Transmisión / Protocolo Internet (Transmission Control Protocol / Internet Protocol). El protocolo de comunicaciones original de Internet. Es el más utilizado en el mundo de las comunicaciones y fue desarrollado bajo las directrices del Departamento de Defensa de los EE.UU.

Trashing:

Obtienen información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos.

Trojan Horse:

Programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema en el que se introduce de manera subrepticia.

Troyano:

Programa que se suele presentar en forma de utilidad gratuita pero que encierra algún malware que abre una puerta dentro del ordenador para que alguien pueda ver datos o tomar el control de nuestro sistema. Muchos programas de seguridad en Internet, incluidos los gratuitos, impiden la entrada de este software malintencionado. Son instrucciones introducidas en la secuencia de instrucciones de otros programas legales (de ahí su nombre) y que realizan funciones no autorizadas, destruyen ficheros o capturan información mientras simulan efectuar funciones correctas. Un caso particular de los troyanos son los salami, generalmente utilizados en instituciones financieras, realizan asientos de pequeñas cantidades, como los redondeos de operaciones de cálculo de intereses, para que no se

detecten por su importancia y al final se transfieren a una cuenta bancaria particular.

Virus:

Programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Se diferencian de los gusanos (ficheros independientes) en que vienen adheridos a otro objeto informático, programa, email, etc. Altera y estropea el buen funcionamiento del ordenador (corrompe o borra los datos guardados en el disco duro, estropea el sistema operativo, etc.). Los virus pueden llegarnos de varias maneras: descargando contenidos de Internet que no sepamos de dónde vienen, abriendo correos electrónicos de procedencia también dudosa, o instalando copias piratas de programas. Los ordenadores con sistema operativo Windows tienen más virus que los que utilizan sistemas operativos Mac o Linux, aunque no existe nada inexpugnable.

Vishing:

Estafa a través del teléfono móvil, utilizando un SMS ‘gancho' para robar datos. Utiliza un mecanismo similar al smishing. El usuario recibe en esta ocasión un mensaje de correo electrónico no demandado, en el que se le solicita que llame inmediatamente a un número telefónico de una determinada empresa. Una vez que realiza la llamada y se pasa esperando los minutos de rigor en estos casos, se le solicitarán datos personales que posteriormente utilizarán sin su autorización.

Vulnerabilidad:

Una falla o debilidad en el diseño, implementación u operación de un sistema que puede llevar a que sea explotado para violar las políticas de seguridad por parte de un intruso.

White Hat:

Hacker que busca los bugs de los sistemas informáticos dando a conocer a las compañías desarrolladoras de software o empresas sus vulnerabilidades, normalmente sin ánimo de perjudicar.

ANEXO 2

CRONOGRAMA DEL PROYECTO

Etapa	Responsable	2015											
		E	F	M	S	M	J	J	A	S	O	N	D
Conocimiento de la importancia de los procesos de seguridad para su implementación.	Equipo de investigación	X	X	X	X								
Capacitar a los responsables del área de informática para proteger la información.	Equipo de investigación					X	X	X	X				
Solo el personal autorizado tenga acceso a los recursos.	Equipo de investigación									X	X	X	X