SERIES DE ESTÁNDARES

GLI-27:

Buenas Practicas en Seguridad de Redes

Versión 1.1

Fecha de Publicación: 21 de Enero del 2013

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Esta página se dejo en blanco intencionalmente

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

ACERCA DE ESTE DOCUMENTO

Este recurso de buenas prácticas de seguridad de redes ha sido producido por **Gaming Laboratories International, LLC** con el propósito de proveer un documento con "buenas prácticas" especifico a la seguridad de redes. Por lo tanto, se espera que este documento sea utilizado como referencia para la seguridad de redes y que no sea visto directamente como un estándar regulatorio.

La seguridad de redes es un tema complejo y varía ampliamente como una función de la red específica y el tipo de datos que es trasportado por esa red. En adición, la escala de la red frecuentemente impacta directamente el nivel y tipo de medidas de seguridad implementados. Por esas razones, las recomendaciones y orientaciones contenidas dentro de este documento no deben ser interpretadas a ser aplicable a cada red ya que cualquier elemento singular de seguridad puede o no ser adecuado. Cada red debe ser evaluada basada en un número de factores como aquellos mencionados antes, y luego desarrollar un plan apropiado para su implementación. Este documento proporciona algún nivel de orientación en términos de las mejores prácticas que existen actualmente y como estas podrían ser aplicadas a una red determinada. La información presentada debe por lo tanto ser vista como ofreciendo consideraciones y no requerimientos.

Este documento de buenas prácticas para la seguridad de red está dirigido a agencias reguladoras, operadores de juego, y proveedores de la industria como una referencia de ayuda para implementar medidas de seguridad en la red. Este documento es en respuesta a las partes interesadas de la industria de juego que han solicitado orientación técnica en el espacio de seguridad de rede. Esta no pretende representar un conjunto de estándares rígidos que todo proveedor y que toda red deba cumplir ya que una talla no encaja en todo el espacio de seguridad de redes.

GLI-27 debe ser visto como un documento con vida que se espera que cambie con la evolución de tecnología y prácticas de seguridad de red.

GLI-27 no está destinado a remplazar o negar cualquier documento presente o futuro de la serie de estándares GLI. Solo como un ejemplo, las recomendaciones de GLI-27 no están destinadas para esquivar cualquier especificación en GLI-21 en caso de que la red en cuestión apoye la funcionalidad de Servidor Cliente. Asimismo para otros tipos de redes y los documentos de estándares GLI que específicamente aplican a ese tipo de redes.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Esta página se dejo en blanco intencionalmente

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Tabla of Contenidos

CAPITULO 1 7
1.0 VISIÓN GENERAL 7
1.1 Introducción 7
1.2 Reconocimiento de Otros Documentos Revisados 8
1.3 Propósito de esta Referencia de Buenas Prácticas 8
1.4 Principios de Diseño de Seguridad de Redes 9
1.5 Definiciones Claves de Seguridad de Red 10
1.6 Operador de Red Clave / Documentación de las Partes Interesadas 17
CAPITULO 2 19
2.0 HARDWARE DE RED 19
2.1 Dispositivos de Red 19
2.2 Controles de Acceso Físico y de Seguridad 22
2.3 Puertos Físicos y Conexiones por Cable 23
2.4 Recuperación de Desastres y Redundancia (Físico) 24
CAPITULO 3 28
3.0 SOFTWARE DE RED 28
3.1 Protocolos y Comunicaciones 28
3.2 Firewalls 29
3.3 Protección de Contraseñas e Inicios de Sesión 32
3.4 Protección de capas-múltiples 35
3.5 Encriptación - Transmisión y Almacenamiento 35
3.6 Conexiones Externas 40
3.7 Programas de Protección para Antivirus y Malware 42
3.8 Parches y Actualizaciones del Software 43
3.9 Recuperación de Desastres (Lógico) 43
3.10 Prevención y Detección de Intrusos 45
3.11 Escaneando Vulnerabilidades 47
3.12 Registro 48
3.13 Acceso Remoto 48
CAPITULO 4 50
4.0 REDES INALÁMBRICAS 50
4.1 Estándares de la Industria 50
4.2 Consideraciones Únicas 50
CAPITULO 5 59
5.0 INGENIERÍA SOCIAL Y EDUCACIÓN 59

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

5.1 Declaración General....59
5.2 Personificación de Vendedores....59
5.3 Información Disponible Públicamente....59
5.4 Seguridad de los Mensajes de Voz....60
5.5 Correo Electrónico Dirigido "Phishing"....60
5.6 Eliminación de Documentos Sensitivos....60

CAPITULO 6 62

6.0 RECURSOS DE CÓMPUTO EN LA NUBE....62

6.1 Declaración General....62
6.2 Consideraciones Generales....62

APÉNDICE 65

Lista de Figuras....65

Figura 1 – Ejemplo de la Topología de una Red con Cableado....65
Figura 2 – Topología para una Red Inalámbrica....66

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

CAPITULO 1

1.0 VISIÓN GENERAL

1.1 Introducción

1.1.1 ***Declaración General***. **Gaming Laboratories International, LLC (GLI)** ha venido ensayado equipos de juego desde 1989. En el transcurso de los años, nosotros hemos desarrollado numerosos estándares para jurisdicciones alrededor del mundo. GLI ha elegido crear este documento como un recurso de buenas prácticas para las agencias reguladoras y operadores de juego como una referencia para implementar medidas de seguridad de red. En años recientes, muchas partes interesadas de la industria de juego han optado por preguntar orientación técnica en el espacio de seguridad de redes. En adición, la tecnología de seguridad de red es de por si compleja y por ello GLI ha visto la necesidad de crear una referencia en un formato familiar para la industria que pueda asistir en la ampliación de su conocimiento de las disciplinas de seguridad de redes. Este documento, estándar GLI-27 establecerá las mejores prácticas en la seguridad de redes.

1.1.2 ***Historia Del Documento***. Este documento está basado en ejemplos de la industria en seguridad de redes, y principalmente estándares técnicos adoptados por el estado de Arizona así como también estándares aplicables definidos por NIST e ISO. Nosotros hemos tomado cada uno de los documentos de los estándares, juntado cada una de las reglas únicas, eliminando algunas reglas y actualizando otras, a fin de reflejar el cambio en tecnología y el propósito de mantener objetividad, una referencia cierta. Nosotros hemos listado a continuación y damos crédito a las agencias cuyos documentos nosotros revisamos antes de escribir este recurso de buenas prácticas. Es la política de **Gaming Laboratories International, LLC** de actualizar este documento lo más seguido posible para reflejar cambios en tecnología, métodos de ensayo, o métodos de hacer trampa. Este documento será distribuido LIBRE DE CARGOS para todos aquellos que lo requieran. Esta referencia y todas las otras pueden ser obtenidas descargándolas

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

de nuestro sitio web www.gaminglabs.com o escribiéndonos a:

Gaming Laboratories International, LLC
600 Airport Road
Lakewood, NJ 08701
(732) 942-3999 Tel
(732) 942-0043 Fax

1.2 Reconocimiento de Otros Documentos Revisados

1.2.1 ***Declaración General***. Estas buenas prácticas han sido desarrolladas de la revisión y usando porciones de los documentos de las organizaciones notadas a continuación donde sea aplicable. Nosotros reconocemos a todos los que ensamblaron estos documentos y les damos las gracias:

a) National Institute of Standards and Technology (NIST) – Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53 Revision 2;
b) National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, NIST Special Publication 800-146
c) State of Arizona, Government Information Technology Agency (GITA) – Network Security, P800-S830 Rev 2.0;
d) International Standards Organization (ISO) International Electro technical Commission (IEC) 27002 and ISO IEC 27005; and
e) "All In One CISSP", CISSP Certification and Exam Guide, by Shon Harris.

1.3 Propósito de esta Referencia de Buenas Prácticas

1.3.1 ***Declaración General***. El propósito de esta referencia de Buenas prácticas es como sigue:

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

a) Crear una referencia para las partes interesadas de la industria de juego interesadas en regular, analizar o certificar redes de juego.

b) Crear una referencia que las partes interesadas puedan utilizar para asegurarse que los sistemas de redes de juego sean seguras y capaces de ser auditadas y operadas correctamente.

c) Construir una referencia que pueda ser fácilmente cambiada o modificada para permitir la introducción de nueva tecnología.

d) Construir una referencia en un formato familiar a las partes interesadas de juego que pueda mejor educarlos en las disciplinas de seguridad de redes.

e) Construir un recurso de buenas prácticas que no especifique un método en particular de seguridad de red. La intención es permitir un rango amplio de métodos a ser usados para cumplir con las buenas prácticas mientras que al mismo tiempo promover el desarrollo de nuevos métodos.

1.3.2 ***No Limitación de Tecnología***. Se debe tener cuidado de que este documento no debe ser leído de forma que limite el uso de tecnología futura. Este documento no debe ser interpretado de que si la tecnología no está mencionada entonces no es permitida. Todo lo contrario, cuando se desarrolle nueva tecnología, nosotros revisaremos esta referencia de buenas prácticas, haremos cambios e incorporaremos los espacios para la nueva tecnología.

1.4 Principios de Diseño de Seguridad de Redes

1.4.1 ***Principios de Diseño de Seguridad de Redes***. Antes de implementar una solución a la seguridad de red, muchos principios claves deben ser considerados. Algunos de estos principios incluyen:

a) **Integridad** que las medidas de seguridad sean preservadas. Estas no deben corromper los datos. Estas deben proteger los datos de una forma consistente todo el tiempo. Estas deben proteger la confidencialidad y sensibilidad de los datos.

b) **Disponibilidad** que las medidas de seguridad estén disponibles todo el tiempo y que los sistemas y datos que se están protegiendo estén disponibles todo el tiempo.

c) **Protección Adecuada** que lo que se está protegiendo sea protegido a un grado

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

proporcional con su valor. Elementos informáticos deben ser protegidos solo has que estos pierdan su valor y ellos deben ser protegidos en un grado consistente con su valor.

d) **Efectividad** que cualquier control que este implementado sea efectivo asegurando la red y las partes de sus componentes. Sin embargo, estos también deben ser eficientes, de fácil uso y apropiados para el tamaño y tipo de organización en los cuales estos operan.

e) **Protección Profunda** que debe ser asumido que un intruso intentara usar cualquier modo de penetración disponible. Esto no necesariamente envuelve los modos más obvios ni es necesariamente en contra de uno que es la defensa mas solida que ha sido instalado.

f) **Debida diligencia** que asegurando la seguridad de la red es un proceso continuo y en evolución. La red debe ser monitoreada y manejada perpetuamente para asegurar su seguridad.

1.5 Definiciones Claves de Seguridad de Red

1.5.1 ***Declaración General***. En la tecnología de la información, una red es una serie de puntos o nudos interconectados por caminos de comunicación. Las redes pueden ser definidas más a fondo por su topología o configuraciones generales. Las redes también pueden caracterizarse en términos de distancia espacial como redes de área local (LAN), y redes de área amplia (WAN). Otras caracterizaciones pueden ser completadas haciendo referencia al tipo de tecnología para la transmisión de datos en uso; ya sea que este lleve voz, datos o las dos clases de señales; por usuarios de la red; por la naturaleza de sus conexiones; y por los tipos de enlaces físicos.

1.5.2 ***Objetivos de la Seguridad de Red***. La seguridad de la red equivale a la protección de redes y sus servicios de modificaciones no autorizadas, destrucción, o divulgación, y provisión de garantía que la red realiza sus funciones críticas correctamente y que todo el software en la red es una copia autentica del software original como lo fue distribuido por su fabricante. La seguridad de la red también ayuda a asegurar la integridad de los datos que atraviesan por la red.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

1.5.3 Definiciones.

Termino	Descripciones
Acceso –	Habilidad para hace uso de cualquier recurso del Sistema de Información (IS).
Autoridad de Acceso –	Una entidad responsable por el monitoreo y permitir privilegios de acceso para otras entidades autorizadas.
Control de Acceso –	El proceso de otorgar o negar pedidos especiales: 1) para obtener y usar información e información relacionada a procesos específicos a una red; 2) para ingresar a facilidades físicas especificas que alojan infraestructura critica de la red.
Seguridad Adecuada –	Seguridad acorde con el riesgo y magnitud de daño que resulte de su pérdida, mal uso, o acceso no autorizado o modificación de la información.
Estándar de Encriptación Avanzado – (AES)	El estándar de encriptación avanzado especifica un algoritmo criptográfico aprobado por el gobierno de los Estados Unidos que puede ser usado para proteger datos electrónicos. El algoritmo AES es un bloque de cifrado simétrico que puede cifrar (encrypt) y descifrar (decrypt) la información. Este estándar especifica el algoritmo Rijndael, un bloque de cifrado simétrico que puede procesar bloques de datos de 128 bits, usando llaves cifradas con longitud de 128, 192, y 256 bits.
Software Contra Virus –	Software usado para prevenir, detectar y remover virus informáticos, incluyendo maliciosos, gusanos y caballos de Troya.
Aplicación –	Software informático diseñado a ayudar el desempeño del usuario en una tarea específica.
Auditoria de Datos –	Registro cronológico de las actividades del sistema que permiten la reconstrucción y exanimación de la secuencia de eventos y cambios en un evento.
Auditoria de Rastreos –	Un registro mostrando quien ha accedido un sistema de tecnología de información y que operaciones el usuario ha realizado durante un periodo dado.
Autenticación –	Verificando la identidad de un usuario, proceso, paquete de software, o dispositivo, usualmente como un pre-requisito para permitir el acceso a recursos en un sistema de información.
Respaldo –	Una copia de los archivos y programas hecha para facilitar su recuperación si fuese necesario.
Plan de Contingencia –	Política y procedimientos de administración diseñados para mantener o restaurar las operaciones de negocio,

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Termino	Descripciones
	incluyendo operaciones informáticas, posibilidad de una locación alternada, en el caso de emergencias, fallas del sistema, o desastre.
Integridad de Datos –	La propiedad de que los datos son ambos, correctos y consistentes y que no han sido alterados en una manera no autorizada. La integridad de los datos cubre los datos su alojamiento, durante proceso, y mientras esta en tránsito.
Zona Desmilitarizada – (DMZ)	Una red insertada en medio de una red privada de la compañía y la red pública externa. Los sistemas que son accesibles externamente pero que necesitan ciertas protecciones están usualmente localizados en las redes DMZ.
Plan de Recuperación de Desastres– (DRP)	Un plan escrito para procesar aplicaciones criticas y prevenir la perdida de datos en caso de un evento mayor de falla del hardware o software o destrucción de las facilidades.
Llave Criptográfica –	Una llave criptográfica que ha sido encriptado usando una función de seguridad aprobada con una llave de encriptación, un PIN, o una clave a fin de ocultar el valor del texto plano subyacente.
Red Ecriptada –	Una red en la cual sus mensajes son encriptados para prevenir que sean leídos por partes no autorizadas.
Encriptación –	Inscripción es la conversión de datos en una forma llamada texto cifrado (ciphertext), el cual no puede ser fácilmente entendido por personas no autorizadas.
Firewall –	Es un mecanismo o dispositivo que limita el acceso entre redes de acuerdo con la póliza de seguridad local
Honeypot –	Un anfitrión que está diseñado como una trampa establecida para detectar, desviar o de alguna manera contrarrestar intentos de uso no autorizado de los sistemas de información y no tiene usuarios autorizados además de sus administradores.
Incidente –	Una violación o amenaza inminente de violación de las pólizas de seguridad informáticas, o prácticas de seguridad informática estándar. Cualquier ocurrencia que actualmente o potencialmente pone en peligro la confidencialidad, integridad, o disponibilidad de un sistema informático o la información de los procesos, almacenamiento, o transmisiones de sistema, o que constituye una violación o amenaza inminente de violación de las pólizas de seguridad, procedimientos de seguridad o pólizas de uso aceptables.
Plan de Respuesta a Incidentes –	La documentación de un determinado conjunto de instrucciones o procedimientos de cuando un ataque

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Termino	Descripciones
	cibernético malicioso es encontrado en contra de los sistemas informáticos de la organización
Sistema de Detección de Intrusos – (IDS)	Software que busca por actividad sospechosa y alerta a sus administradores.
Sistemas de Prevención de Intrusos –	Sistemas que pueden detectar una actividad intrusiva y que puede también tratar de parar la actividad idealmente antes que esta alcance sus objetivos.
Dirección IP –	Una dirección IP es un número único para una computadora que es usado para determinar donde los mensajes que son transmitidos en el internet deben ser entregados. La dirección IP es análoga al número de una casa para el correo postal ordinario.
Seguridad IP – (IPSec)	IPsec es un conjunto de protocolos para asegurar las comunicaciones del protocolo de internet (IP) autentificando y encriptando cada paquete IP de un flujo de datos. IPsec también incluye protocolos para establecer autentificación mutua entre agentes al inicio de la sesión y negociación de llaves criptográficas a ser usadas durante la sesión. IPsec es un estándar del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE), Pedido de Comentarios (RFC) 2411, protocolo que provee capacidad de seguridad al protocolo de internet (IP) capa de comunicaciones. Administración de llaves del protocolo IPsec es usado para negociar las llaves secretas que protegen la comunicación de la Red Virtual Privada (VPN), y el nivel y tipo de protecciones de seguridad que caracterizaran la VPN. El más amplio protocolo de administración de llaves usado es el protocolo de Intercambio de Llaves de Internet (IKE).
Kerberos -	Es protocolo de autenticación de red diseñado para proveer una fuerte autenticación para aplicaciones cliente/servidor usando criptografía de llave secreta.
Llave –	Es un valor usado para controlar las operaciones criptográficas como des-encriptación, encriptación, generación de firmas o verificación de firma.
Software Malicioso (Malware) –	Es un programa que es insertado dentro de un sistema usualmente encubierto con el intento de comprometer la confidencialidad, integridad, o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima o de cualquier otra molestia o interrupción a la víctima.
Código Mensaje de Autenticación – (MAC)	Es una suma de verificación (checksum) criptográfica para detectar ambas, modificaciones de datos accidentales e intencionales.
No-repudiación –	Certeza de que el emisor de la información es provisto con una prueba de entrega y el receptor es provista con prueba

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Termino	Descripciones
	de la identidad del emisor, de manera que ninguno pueda luego negar el haber procesado la información.
Contraseña Password –	Un secreto que el peticionario memoriza y usa para autentificar su identidad. Los passwords son típicamente cadenas de caracteres. Una cadena de caracteres protegida y usada para autenticar la identidad del usuario del sistema de cómputo o autorizar acceso a recursos del sistema. Una cadena de caracteres (letras, números, y otros símbolos) usados para autenticar una identidad o para verificar la autorización de acceso.
Número de Identificación Personal– (PIN)	Es un clave que consiste solamente de números decimales. Es un número secreto que el peticionario memoriza y usa para y usa para autenticar su identidad. Los PINS son generalmente números decimales. Es un código alfanumérico o clave usado para autenticar una identidad.
Phishing –	Es engañar a individuos a revelar información personal sensitiva mediante métodos informáticos engañosos.
Póliza (para la Seguridad) –	Es un documento que delinea la estructura de manejo de la seguridad y claramente asigna responsabilidades de seguridad y pone la fundación necesaria para confiablemente medir su progreso y cumplimiento.
Puerto –	Es un punto físico de entrada o salida de un modulo criptográfico que provee acceso al modulo para señales físicas representado por el flujo de información lógica (puertos separados físicamente no comparten el mismo pin físico o cableado).
Llave Privada –	La parte secreta de un par de llaves asimétricas que es usado típicamente para firmar digitalmente o des-encriptar datos. Encriptación con **llave Asimétrica** usa diferentes llaves para la encriptación y des-encriptación. Estas dos llaves son matemáticamente relacionadas y estas forman un par de llaves.
Proxy –	Un proxy es una aplicación que "rompe" la conexión entre el cliente y el servidor. El proxy acepta ciertos tipos de trafico ingresando o dejando una red, los procesa y los re-envía. Esto cierra efectivamente la ruta directa entre las redes internas y externas. Haciendo así mas difícil para un atacante de obtener direcciones internas y otros detalles de la red interna de la organización. Servidores proxy están disponibles servicios comunes de internet; por ejemplo, un Protocolo de Transferencia de Texto Hyper (HTTP) proxy usado para acceso web, un Protocolo de Transferencia de

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Termino	Descripciones
	Correo Simple (SMTP) proxy usado para e-mail.
Llave Publica –	Es la parte pública de un par de llaves asimétricas que es típicamente usado para verificar firmas o encriptación datos.
Acceso Remoto –	Acceso por usuarios (o sistemas de información) comunicándose externo a un perímetro de seguridad del sistema de información.
Riesgo –	Es la posibilidad de que una amenaza tenga éxito en su ataque en contra de la red.
Protocolo de Comunicación Seguro –	Un protocolo de comunicación que provee apropiada confidencialidad, autenticación y protección de integridad del contenido.
Ingenieria Social –	Es un truco que alguien utiliza para hacer revelar información (por ejemplo una clave) que puede ser usado para atacar los sistemas o redes.
Amenaza –	Cualquier circunstancia o evento con el potencial de adversamente impactar las operaciones de la red (incluyendo misión, función, imagen o reputación), bienes o individuos mediante un sistema de información vía acceso no autorizado, destrucción, divulgación, modificación de información, y/o servicio denegado. También, la posibilidad de una amenaza de código de explotar con éxito la vulnerabilidad de un sistema de información en particular. Una amenaza es cualquier posibilidad de peligro para una red que alguien o algo pueda ser capaz de identificarse como vulnerable y que por tanto busque ser explotada.
Acceso No-Autorizado –	Una personal logra acceso físico o lógico sin permiso a una red, sistema, aplicación, datos u otros recursos.
Verificación y Validación	Asegurado por verificación de firmas electrónicas que cualquier paquete de software es una copia autentica del software creado por su fabricante y si es aplicable, una copia exacta del software certificado por el ITL. Los estándares para la validación y verificación son discutidos dentro de otros estándares GLI aplicables.
LAN Virtual– (VLAN)	Una red virtual LAN (VLAN) es un grupo de anfitriones (host) con un conjunto común de requerimientos que se comunican como si estuvieran adjuntas al mismo dominio de difusión a pesar de su locación física. Una VLAN tiene los mismos atributos que una LAN física, pero esta permite que terminales destinatarias estén agrupadas juntas aun si ellas no están localizadas en el mismo conmutador de red. VLANs son implementadas al añadir un encabezado a cada cuadro que contiene “etiquetas” para identificar a que LAN

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Termino	Descripciones
	el cuadro pertenece.
Red Virtual Privada – (VPN)	Una red virtual privada es una red lógica que es establecida sobre una red física existente y que típicamente no incluye cada nodo presente en la red física.
Virus –	Es un programa de auto-replica, típicamente con intentos maliciosos que funciona y se esparce modificando otros programas o archivos.
Vulnerabilidad –	Software, hardware, u otra vulnerabilidad en la red que puede proporcionar una "puerta" para introducir la amenaza.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

1.6 Operador de Red Clave / Documentación de las Partes Interesadas

1.6.1 ***Identificación de riesgos.*** No hay un sistema seguro completo. Por lo tanto, es necesario definir que porciones del negocio requieren la mayor cantidad de recursos dirigidos a la seguridad. Cada unidad discreta en una organización tendrá alguna porción de su funcionalidad básica dependiente en la información tecnológica y debe ser una parte de interés. Cada parte de interés debe ser capaz de definirse con funciones específicas que están en riesgo desde la perdida de datos, manipulación, o filtración. Esto puede ser considerado a ser el primer paso en un análisis de riesgo que debe ser usado como una base de las pólizas de seguridad de la información.

1.6.2 ***Pólizas de Seguridad de la Información (prevención).*** Una póliza de seguridad detallada (de aquí en adelante "la póliza") es requerida a identificar, documentar, y dar soporte a las muchas facetas de seguridad de la red descritas a lo largo de este documento. El desarrollo de la póliza debe ser predicado sobre el rendimiento de detallado análisis de riesgo. El documento de la póliza debe ser desarrollado, implementado y mantenido por los operadores de la red / partes interesadas y debe:

a) Estar formalmente documentado y regularmente revisado.

b) Define las expectaciones y responsabilidades de los empleados, y establece consecuencias por el fallo de seguir la póliza, y adicionalmente:

   i. Define los roles y responsabilidades dentro de la organización para la seguridad de la información.

   ii. Fija la visión de la alta gerencia en relación a la seguridad.

   iii. Define os requerimientos de protección de acuerdo con la evaluación del riesgo.

   iv. Incorpora entrenamientos para conciencia de los empleados, lo que debería ser hecho al tiempo de su contratación y luego anualmente.

1.6.3 ***Póliza de Respuesta de Incidentes (respuesta).*** Una póliza de Respuesta de Incidentes (IRP) es esencial para asegurar que las amenazas a la seguridad de la red son respondidas

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

en un tiempo y de manera efectiva en caso de que medidas preventivas fallen o estén comprometidas. Un documento IRP detallado debe ser desarrollado, implementado, y mantenido por el operador de la red / partes interesadas y deben:

a) Estar formalmente documentados y ensayados anualmente
b) Definir roles y responsabilidades durante un incidente.
c) Definir un plan de comunicaciones para ambos interno y externo (prensa).

1.6.4 ***Plan De Recuperación de Desastres (recuperación)*** Practicas y procedimientos de alto nivel deben ser establecidos para ayudar en el evento de falla de la infraestructura critica y ayudar a controlar el daño en caso de que las medidas preventivas de la seguridad de red fracasen de proteger un ataque. Un documento detallado Plan de Recuperación de Desastres (DRP) debe ser desarrollado, implementado, y mantenido por el operador de la red / partes interesadas y debe asegurar que:

a) El personal está entrenado y familiar con los procedimientos relacionados.
b) El respaldo de datos es realizado y mantenido y enviado fuera del sitio en intervalos regulares (preferible diariamente).
c) Centros de Datos múltiples están diseñados dentro de las operaciones de la red.
d) Sistemas de alta disponibilidad son utilizados efectivamente quienes mantienen ambos los datos y el sistema replicado fuera del sitio.

Nota Especial: *Un plan de recuperación de datos es visto como la principal responsabilidad del operador de red versus algo que un proveedor de redes es responsable. Con eso dicho, cualquier DRP creíble debe involucrar y utilizar la experiencia y conocimiento que el proveedor de la red tiene que ofrecer. Adicionalmente, no todas las redes requieren el desarrollo y mantenimiento de un DRP formal ya que estas pueden ser de pequeña escala, red no sofisticada que transportan datos de baja sensibilidad. Controles internos del operador de red deben dictar la necesidad de un DRP sujeto al tipo de red en uso y la naturaleza de los datos que son transmitidos sobre esa red.*

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

CAPITULO 2

2.0 HARDWARE DE RED

2.1 Dispositivos de Red

2.1.1 ***Tipos de Dispositivos de Red.*** La tabla a continuación resume brevemente una variedad de dispositivos de red comúnmente usados en redes de estos días modernos.

TABLA 2.1.1 – RESUMEN DE LOS DISPOSITIVOS DE RED

Dispositivo	Función/Propósito	Puntos Claves
Hub	Conecta dispositivos en una red de pares-cruzados.	Un hub no realiza cualquier función aparte de la regeneración de señal.
Conmutador (Switch)	Conecta dispositivos en una red 802.3.	Un conmutador re-envía los datos a su destinación usando la dirección MAC integrada en cada paquete.
Puente (Bridge)	Divide la red para reducir el tráfico en general de la red.	Un puente permite o previene que los datos pasen por este leyendo la dirección MAC.
Enrutador (Router)	Conecta a redes juntas.	Un enrutador usa el software-configurado con la dirección de la red para hacer decisiones de re-envío.
Gateway	Traduce de un formato de datos a otro.	Los gateway pueden ser basados en hardware o software. Cualquier dispositivo que traduce el formato de datos es llamado un gateway.
Unidad de Canales de Servicio / Unidad de Servicios Digitales (CSU/DSU)	Traduce las señales digitales usadas en una LAN a aquellas usadas en una WAN.	La funcionalidad CSU/DSU esta algunas veces incorporada dentro de otros dispositivos como un enrutador con una conexión WAN.

Derechos de Autor ☐ 2013 Gaming Laboratories International, LLC
Todos los Derechos Reservados.

Dispositivo	Función/Propósito	Puntos Claves
Tarjeta de Interface de Red (NIC)	Habilita la computadora terminal y sistemas para conectarlos a la red.	Las interfaces de red pueden ser tarjetas de expansión complementarias, tarjetas PCMCIA, o interfaces incorporadas.
Adaptadores de terminales de Servicios Integrados de Red Digital (ISDN).	Conecta los dispositivos a líneas ISDN.	ISDN es una tecnología WAN digital utilizada a menudo en lugar de enlaces modem lentos. Los adaptadores terminales ISDN son requeridos para reformatear el formato de los datos para transmisiones en enlaces ISDN.
Sistema de tarjeta de red de área	Usado en un grupo de servidores para proveer conectividad entre nodos.	Los sistemas de tarjeta de red de área son dispositivos de alto rendimiento capaces de hacer frente las demandas de aplicaciones de grupo.
Punto de acceso inalámbrico (WAP)	Provee funciones de red a dispositivos de red inalámbricos.	Un WAP es utilizado con frecuencia para conectar a una reda alambica de ese modo actúa como un enlace entre las porciones de cabreado e inalámbricas de la red.
Modem	Provee comunicaciones seriales a través de líneas telefónicas.	Los Módems modulan la señal digital en una análoga en el lado del emisor y realiza la función reversa en el lado de recepción.

2.1.2 Descripciones Claves de los Dispositivos de Red.

a) **Hubs:** Los hubs son los dispositivos de red más simples y simplifican la difusión de la misma información a todos los puertos conectados incluyendo los puertos originarios. En un hub, los datos son reenviados a todos los puertos, sin importar que los datos sean destinados para el sistema conectado al puerto. Las computadoras se conectan al hub vía un largo cableado de pares-cruzados. En adición a los puertos para conectar las

Derechos de Autor ☐ 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

computadoras, muchos hubs tienen un puerto diseñado como puerto uplink que habilita al hub a ser conectado con otro hub para crear una red más grande.

b) **Conmutador (Switches):** A superficie, un conmutador luce my parecido a un hub. Múltiples conmutadores pueden ser utilizados como los hubs para crear redes más grandes. A pesar de ser similares en apariencia y sus idénticas conexiones físicas a computadoras, los conmutadores ofrecen ventajas operaciones significantes sobre los hubs. En vez de reenviar los datos a todos los puertos conectados, un conmutador reenvía los datos solamente al puerto al cual el sistema destinatario está conectado. Este mira en las direcciones del Control de Acceso al Medio (MAC) de los dispositivos conectados a este para determinar el puerto correcto. Una dirección MAC es un número único que está programado dentro de todo NIC. Al reenviar los datos solamente al sistema para el cual los datos están dirigidos, el conmutador disminuye la cantidad de tráfico dramáticamente en cada enlace de red. En efecto, el conmutador canaliza o cambia los datos entre los puertos.

c) **Puentes (Bridges):** Los puentes son dispositivos de red que dividen redes. Un puente funciona bloqueando o reenviando información basada en la dirección MAC escrita dentro de cada marco de datos. Si el puente cree que la dirección de destino está en una red distinta a la cual donde el dato fue recibido, este puede reenviar los datos a otras redes al cual este está conectado. Si la dirección no está al otro lado del puente, el paso de los datos es bloqueado. Los puentes "aprenden" las direcciones MAC de los dispositivos en las redes conectadas "escuchando" al tráfico de la red y registrando la red de donde el trafico se origina. Las ventajas de los puentes son simples y significantes. Al prevenir que el trafico no necesario cruce a otros segmentos de la red, un puente reduce dramáticamente la cantidad de tráfico en un segmento. Los puentes también hacen posible aislar una red ocupada de una no tan ocupada, evitando así la contaminación de nodos ocupados. Cuando un punto de acceso inalámbrico permite la comunicación entre clientes inalámbricos y clientes cableados, entonces este actúa como un puente entre estas dos redes.

d) **Enrutadores (Routers):** Los enrutadores son dispositivos de red que literalmente dirigen los datos entre la red de computadoras más allá de los dispositivos conectados

Derechos de Autor □ 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

directamente. Examinando los datos en cuanto estos arriban, el enrutador es capaz de determinar la dirección de destino de los datos; luego usando tablas de enrutadores definidas, el enrutador determina la mejor vía para que los datos continúen su jornada. Distinto de los puentes y conmutadores que usan las direcciones MAC configuradas en el hardware para determinar la destinación de los datos, los enrutadores usan las direcciones de red configuradas en el software para hacer las decisiones.

e) **Gateways:** El termino Gateway es aplicado a cualquier dispositivo, o aplicación software que pueda realizar la función de traducir datos de un formato a otro. La funcionalidad clave de un Gateway es que este convierte el formato de los datos y no los datos a sí mismos.

f) **Puntos de Acceso Inalámbrico (WAP's):** Los WAP son dispositivos parecidos al hub, típicamente con una antena. Estas permiten la conectividad vía una interface aérea. Un WAP sirve como un enlace entre las porciones con cableado e inalámbricas de una red.

g) **Módems:** Los módems realizan una función simple: Ellos traducen las señales digitales de una computadora en señales análogas que pueden viajar mediante líneas de teléfono convencional. El modem modula la señal en el lado desde donde se envía y lo de-modula en el lado donde se recibe. Los módems proveen un método de comunicación relativamente lento.

h) **Tarjeta de Interface de Red (NIC's):** Las tarjetas de interface de red (NIC's), algunas veces llamadas simplemente tarjetas de red, son los mecanismos por el cual las computadoras de conectan a una red.

2.2 Controles de Acceso Físico y de Seguridad

2.2.1 ***Declaración General***. La seguridad física equivale a la habilidad de permitir o negar el uso de un recurso particular por una entidad particular a través de maneras físicas y tangibles. La seguridad física es un importante componente de la protección de cualquier red. Controles de acceso físico son facciones de seguridad que controlan como los usuarios y los sistemas se comunican e interactúan con otros sistemas y recursos, y estos sirven para proteger los sistemas y

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

recursos de acceso no autorizado. Seguridad física de la red debe abordar las áreas claves de robo, sabotaje, vandalismo, accidentes y calamidades del medioambiente y/o naturales.

2.2.2 Acceso al Cuarto del Servidor.

a) Acceso no autorizado al cuarto de servidores debe ser prevenido con la implementación de puntos de entrada con llave y/o un sistema de tarjetas, o mecanismo similar, capaz de registrar y/o controlar todas las entradas a los cuartos en los cuales están presentes sistemas alojando información sensitiva. Algunos cuerpos reguladores requieren dos factores de autenticación.

b) Los registros deben ser revisados rutinariamente por cualquier anomalía en los patrones de acceso.

2.2.3 Seguridad de Estantes/Gabinetes del Servidor.

a) Los estantes/gabinetes deben estar asegurados con llave para crear una barrera física para acceder a los servidores.

b) Acceso a los estantes/gabinetes debe estar restricto solo para empleados autorizados.

2.3 Puertos Físicos y Conexiones por Cable

2.3.1 Seguridad del Enchufe de la Red.

a) El enchufe de la red debe estar deshabilitado cuando no está en uso. Esto puede ser por:

b) Desconexión física (brecha aérea)

c) Administrativo, tal como la asignación a una especial VLAN “muerta”

d) Instalando en una caja con llave un toma de enchufe.

e) Un registro de los enchufes de red habilitados debe ser mantenido y regularmente auditado.

Derechos de Autor ☐ 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

f) Peticiones y aprobaciones para la activación de los enchufes debe ser registrado por el personal de tecnología de la información (IT)

2.3.2 Dispositivos de Red.

a) En el caso de dispositivos de red que no se encuentran en el cuarto de servidores, el acceso a los dispositivos de red (enrutadores, firewalls, conmutadores, etc.) debe ser restringido solo a empleados autorizados.

b) Dispositivos de red deben alojarse en un ambiente seguro.

2.3.3 Servicios y Puertos no Necesarios.

a) Los dispositivos de red deben tener apagados los servicios no necesarios/no usados y deshabilitados los puertos no esenciales. (NOTA: El proveedor de la red debe ser consultado antes de la desactivación de cualquier servicio o puerto para asegurar que algún servicio/puerto no sea involuntariamente desactivado. Por ejemplo, muchos servicios esenciales solamente funcionan esporádicamente, de modo que su uso mismo no es siempre una medida confiable de importancia.)

b) Diseño apropiado y construcción de la red deber ser seguido para todas las nuevas configuraciones de red para asegurar que los apropiados controles de seguridad sean implementados.

2.4 Recuperación de Desastres y Redundancia (Físico)

2.4.1 Recuperación de Desastres. Redundancia de red implica en hacer disponible los recursos en caso de fallos y hacer que esos recursos sean disponibles con la mayor fluidez posible y con poca interacción manual en caso de que estos sean necesarios. Recuperación de desastres significa tener un plan en caso de fallos catastróficos para retornar rápidamente acceso a los

Derechos de Autor ☐ 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

recursos. La red debe utilizar uno o más de los siguientes elementos para apoyar la recuperación de desastres y redundancia:

a) Hardware Redundante – La red debe utilizar múltiples partes de hardware como por ejemplo NIC's que operan paralelamente. En caso que uno falle, el otro continuara la función.

b) Alta-Disponibilidad – La red debe emplear múltiples partes de hardware como por ejemplo enrutadores que son idénticos y configurados de manera que si el componente hardware primario falla, el otro secundario se hará cargo con poca o ninguna interacción administrativa.

c) Hardware Intercambiable / Repuestos Fríos – Copias exactas del hardware deben ser mantenidas, de manera que en caso de fallo, el hardware puede ser intercambiado rápidamente o remplazado. Esto incluye hardware que no está completamente configurado en una capacidad de trabajo, pero que puede ser tomado del inventario, configurado, e implementado en la red en un plazo bastante corto en caso de falla del componente. Esto reduce o elimina el tiempo de inactividad asociado con la reparación del componente hardware original y configurando un remplazo nuevo.

d) Reflejando – La red debe utilizar la reflexión. La reflexión típicamente aplica al almacenamiento de datos y es el proceso de tener todos los datos, incluyendo cambios, replicados a una locación secundaria en tiempo real. Este proceso de replicación permite ya sea un intercambio de hardware o la restauración de datos en caso de una falla.

e) Centros de Copia de Seguridad de Datos – La red debe emplear múltiples centros de datos o sitios, es decir un sitio primario y secundario. El sitio secundario puede ser utilizado en caso de una emergencia mayor y/o desastre natural u otra calamidad en el sitio primario.

    i. Sitio de Reserva en Frio (Cold Backup Site) – El menos caro pero el que consume más tiempo. Un sitio de reserva en frio es nada más que un espacio configurado-apropiadamente dentro del local. Todo lo necesario para restablecer el servicio de red debe ser adquirido y entregado.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

ii. Sitio de Reserva Templado (Warm Backup Site) – Un sitio que ya esta bastecido con hardware representando un duplicado razonable de lo que se encuentra en el sitio primario. Típicamente, los respaldos de datos más recientes deben ser entregados y una restauración debe ser realizada.

iii. Sitio de Reserva Caliente (Hot Backup Site) – El más caro pero el más rápido para la recuperación. Un sitio caliente generalmente contiene una reflexión virtual del sitio actual con los sistemas esenciales listo para ser activado en cualquier momento.

En relación a los centros de respaldo de datos, el término "sitio" se puede referir al espacio físico donde está colocado o geográficamente separado. Separación geográfica puede ofrecer la mayor seguridad, redundancia y sobrevivencia pero esta también viene con un gasto más elevado. Por lo tanto, esta es una decisión de negocios que el operador de la red debe evaluar en conjunto con la red específica y datos involucrados.

2.4.2 ***Plan de Recuperación de Datos***. – Como lo descrito anteriormente en este documento, un plan de recuperación de datos (DRP) debe documentar cuidadosamente todos los métodos que son utilizados para apoyar la recuperación de desastres de la red. Este plan también debe documentar información de contacto esencial y debe detallar los pasos requeridos que afectan una recuperación total de la red. Todos los miembros claves y alta gerencia deben tener múltiples formas de acceso al documento DRP en ambas formas, electrónica e impresa, y el plan debe ser revisado frecuentemente para tratar los cambios a los sitios, equipo, procedimientos y personal.

2.4.3 ***Respaldo de Red (Network Backup)***. Los siguientes elementos para el respaldo de información son requeridos para asegurar la seguridad de la red:

a) Los niveles necesarios de información de respaldo deben ser definidos en un plan de recuperación de desastres documentado;

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

b) Registros precisos y completos de las copias de seguridad y procesos de restauración documentados deben ser producidos;

c) La cantidad (por ejemplo, completo respaldo diferencial) y frecuencia de los respaldos debe reflejar los requerimientos de la organización, los requerimientos de la información involucrada, y lo critico de la información para la operación continua de la organización;

d) Los respaldos deben ser guardados en una locación remota, a una distancia suficiente para escapar a cualquier daño de un desastre en el sitio principal pero que se mantenga recuperable a tiempo para mantener la disponibilidad de datos;

e) La información de respaldo debe ser dada un nivel apropiado de protección física y ambiental consistente con los estándares aplicados al sitio principal; los controles aplicados a los medios en el sitio principal deben ser extendidos a cubrir el sitio donde están los respaldos;

f) Los medios de respaldo deben ser probados regularmente para asegurarse que estos pueden ser confiables en caso se requiera su uso cuando sea necesario;

g) Los procedimientos de restauración deben ser regularmente probados para asegurar que estos son efectivos y que estos pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación;

h) En situaciones donde la confidencialidad es de importancia, los respaldos deben ser protegidos mediante encriptación. A pesar de que NIST no requiere específicamente encriptación de respaldo, estos mantienen estándares para la encriptación de los datos guardados, y los datos de respaldo pueden ser vistos como una extensión de eso.

Nota Especial: *Recuperación de desastres, un plan de recuperación de desastres y respaldo de red debe ser evaluado en el contexto de la red en cuestión. Algunas redes no requieren uno o más de estos métodos. Un análisis de riesgo apropiado debe ser realizado para la red en conjunto con el análisis de costo-beneficio para determinar que método se necesita y a que extensión es financiablemente prudente.*

Derechos de Autor ☐ 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

CAPITULO 3

3.0 SOFTWARE DE RED

3.1 Protocolos y Comunicaciones

3.1.1 ***Protocolos de Red***. Esta sección resume los protocolos de red comúnmente-usados. Los protocolos específicos que son apropiados para la implementación en una red dada esta más allá del alcance de este documento. De cualquier manera, el protocolo de control de transmisiones/protocolo de internet (TCP/IP) es un protocolo dominante usado en la mayoría de redes modernas de estos días.

a) UUCP (UNIX-a-UNIX Protocolo de Copia) – Es un conjunto de programas Unix usados para enviar archivos entre diferentes sistemas Unix y para enviar comandos a ser ejecutados en otro sistema.

b) TCP/UDP – Protocolos de métodos de transporte utilizados como parte conjunto de protocolos TCP/IP. TCP asegura que los datos arriben intactos y completos, mientras UDP solamente envía hacia afuera paquetes. TCP es usado para todo lo que tiene que arribar en forma perfecta y UDP es usado para funciones como transmitir media y video conferencia donde es imposible de transmitir paquetes perdidos.

c) SNMP (Protocolo de Administración de Red Simple) – Ampliamente usado protocolo de monitoreo y control de red que es parte del conjunto de protocolos TCP/IP. Los agentes SNMP recopilan y analizan los datos que se pasan para descubrir y analizar patrones de tráfico.

d) RMON (Monitoreo Remoto) – Mejoras al protocolo SNMP que suma un conjunto comprensivo de funciones de monitoreo de red y permite mucha más información acerca de la red sea pasada a una locación remota.

e) DHCP (Protocolo de Configuración de Anfitrión (host) Dinámico – Es una función en ambos, software y el sistema operativo de la mayoría de hardware que permite

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

automáticamente que las direcciones IP asignadas temporalmente sean asignadas bajo petición.

f) FTP (Protocolo de Transmisión de Archivos) – Es un protocolo usado ampliamente para mover archivos a través de redes desconocidas o heterogéneas.

3.1.2 Comunicaciones Seguras.

a) Todas las comunicaciones confidenciales deben emplear alguna forma de encriptación que haya sido aprobado por el operador de la red / partes interesadas.

b) Toda comunicación de datos confidenciales debe incorporar un esquema de detección y corrección de errores aprobado por el operador de la red / partes autorizadas para asegurar que los datos son transmitidos y recibidos con exactitud.

c) La red debe ser capaz de detectar y mostrar ciertas condiciones. Estas condiciones deben constar en un registro de errores que puede ser mostrado o imprimido a petición, y debe archivar las condiciones por un mínimo de noventa (90) días:

   i. Restablecimiento de energía o falla de cualquier componente de la red.

   ii. Perdida de comunicaciones entre cualquier componente de la red.

   iii. Falla de autenticación. Esta puede ser ya sea una falla al inicio de sesión o falla de intercambio de llaves.

3.2 Firewalls

3.2.1 Declaración General. Un firewall es simplemente un grupo de componentes que colectivamente forman una barrera entre dos redes. La implementación de firewall adecuadas es altamente *recomendada.* Los siguientes requerimientos claves deberían aplicar a un firewall:

a) Tecnología Firewall debería ser implementada en los bordes de la red para proteger en contra del acceso no autorizado a información interna de los bienes.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

b) Todo trafico externo y de zona desmilitarizada debe ser dirigido a través de los dispositivos de firewall. Reglas de tráfico de red deben ser aplicadas en línea con el diseño operacional.

c) Reglas del trafico de red deben incluir pero no se limitan a los siguiente:

   i. Permitir el monitoreo del estado de conexión.

   ii. Un paquete entrante no debe tener una dirección de origen de la red interna,

   iii. Un paquete entrante no debe contener tráfico de protocolo de control de mensajes de internet (ICMP).

   iv. Un paquete entrante debe tener una dirección de destino publica registrada asociada con la red interna si se está usando un traductor de direcciones de red (NAT) estático o dinámico.

   v. Un paquete saliente debe tener una dirección de origen de la red interna,

   vi. Un paquete saliente no debe tener una dirección de destino de la red interna,

   vii. Un paquete entrante o saliente no debe tener una dirección de origen o destino que sea privada o en un espacio reservado,

   viii. Fuentes de tráfico desde sitios de internet que son conocidos por contener correo no deseado (spam), material ofensivo, etc., deberían ser preferiblemente bloqueados.

   ix. Cualquier fuente de paquetes dirigidos o cualquier paquete con opciones establecidas en el campo de protocolo de internet (IP) debe ser bloqueado.

   x. Trafico entrante o saliente conteniendo la dirección de origen o destino de 127.0.0.1 ó 0.0.0.0, enlace local (169.254.0.0 - 169.254.255.255), o direcciones de difusión dirigidas deben ser bloqueadas.

d) Cuando se requiera permitir servicios tales como voz (Voz sobre IP – VoIP), mensajería instantánea, presencia, servicios de movilidad, multimedia (Multimedia sobre IP – MoIP), etc., para atravesar con seguridad los bordes de la red y funcionalidad NAT, las tecnologías firewall deben incluir las siguientes reglas adicionales:

   i. Uso de una sesión de iniciación de protocolo (SIP) de servido proxy ó portero H.323 fuera del firewall, con el firewall configurado para permitir comunicaciones de puntos de destino solamente con el servidor proxy, o

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

ii. Estar configurado para funcionar como portero de las capas de aplicación que monitorean todo trafico SIP y H.323 para abrir y cerrar puertos restringidos como se requiera y re-escribir las direcciones IP dentro la capa de aplicación de mensajes no cifrados, o

iii. Usar una sesión de control de borde (SBC), también conocida como una aplicación enrutador que permite comunicaciones VoIP de extremo a extremo a través de múltiples redes IP mientras permite que puntos destinatarios VoIP como lo son porteros VoIP, teléfonos IP, y teléfonos IP soft; los cuales están detrás de un firewall traductor de direcciones de red (NAT), para comunicarse con puntos destinatarios VoIP en redes IP externas.

e) Los borradores propuestos por el Grupo de Trabajo de Ingeniería del Internet (IETF) para NAT transversal como lo es la Conexión Orientada al Medio de Transporte, Comunicaciones de media caja (Midcom), Transversal Simple de UDP a través de NAT (STUN), Transversal Usando NAT Relay (TURN), cuando se tome singularmente, no provee una solución completa, comprensiva. IETF borrador de internet del Establecimiento de Conectividad Interactiva (ICE) es una metodología propuesta para NAT transversal por SIP. ICE hace uso de protocolos existentes como STUN, TURN y también ámbito especifico IP (RSIP). ICE trabaja a través de la cooperación de ambos puntos extremos en unas sesión.

f) Tecnologías de administración remota de firewall deben ser mediante comunicaciones cifradas o no permitidas en su totalidad.

g) Pólizas del Firewall deben ser revisadas, ensayadas y auditadas con una determinada frecuencia y documentados por el operador de la red / partes interesadas.

3.2.2 ***Múltiples Redes***. En caso de que el servidor de una red en particular es usado en conjunto con otras redes, todas las comunicaciones, incluyendo acceso remoto deben pasar por lo menos un nivel de aplicación de firewall aprobado y no debe tener la facilidad de permitir un camino de red alterno. I existe un camino de red alterno para propósitos de redundancia, este también debe pasar por lo menos un nivel de aplicación de firewall.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

3.2.3 ***Reportes de Auditoria del Firewall***. La aplicación firewall debe mantener un reporte de auditoría de la siguiente información y debe deshabilitar todas las comunicaciones y generar un evento de error si la capacidad del reporte de auditoría se llena:

a) Todos los cambios de configuración del firewall;

b) Todos los intentos de conexión exitosos y sin éxito* a través del firewall; el numero de intentos de conexión fallidos debe ser un parámetro configurable por el operador de la red y partes interesadas; y

c) Direcciones IP de origen y destino y los números de puertos para ingresar el trafico; y
Nota: En casos donde un firewall NAT no tiene la capacidad de registrar la dirección IP de destino si se encuentra en su tabla de re-envío NAT, el registro de la dirección IP de destino no es necesario.

d) Direcciones MAC para el tráfico saliente. Por lo menos, la conexión inicial con éxito con una dirección MAC nueva.

** Por favor note, un parámetro configurable, "intentos de conexión fallidos", puede ser utilizado para denegar pedidos de conexión futura en caso de que el parámetro definido se exceda. El operador de la red / partes interesadas también deben ser notificados.*

3.3 Protección de Contraseñas e Inicios de Sesión

3.3.1 ***Dispositivo de contraseñas y configuraciones***.

a) Dispositivos de contraseñas deben ser cambiados inmediatamente antes o luego de la instalación del dispositivo y debe conformar con los requerimientos establecidos por la póliza de seguridad de la red;

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

b) Los dispositivos de red deben ser configurados para retener su configuración actual, configuraciones seguridad, contraseñas, etc., durante un proceso de reinicio o restablecimiento;

c) Todas las contraseñas administrativas debe ser cambiado regularmente (se recomienda cada 45 días), o por lo menos, en cualquier momento en que el personal de IT deja la organización. El envejecimiento de contraseñas es altamente *recomendado*;

d) Solamente cuentas individuales que están únicamente atadas a un individuo deben ser utilizadas – no compartidas o cuentas genéricas deben ser usadas excepto para aquellas usadas para acceso solo de lectura como se describe en otras partes de este documentos;

e) El acceso para empleados despedidos o suspendidos debe ser removido dentro de 24 horas de la notificación;

f) El acceso para empleados que has sido transferidos a otros departamentos debe ser removido en casos donde las nuevas funciones del empleado no son mas relacionadas con los privilegios de acceso previos;

g) Parámetros deben ser configurables para permitir solo un cierto número de intentos fallidos de inicio de sesión dados por la contraseña de cierto usuario. Una vez que el parámetro se excede, la cuenta debe requerir intervención administrativa para desbloquear*; y

**Por favor note que los bloqueos de cuenta pueden ser a si mismo influencia de ataque de Negación de Servicio.*

NOTA: *GLI **recomienda** los siguientes criterios mínimos de contraseñas:*

1) 8 – 14 caracteres de largo;
2) Una combinación de por lo menos tres de los siguientes componentes:
   Letras mayúsculas
   Letras minúsculas
   Números
   Caracteres especiales
3) No ser parte del nombre de inicio de sesión;

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

4) No ser parte de una contraseña previa (por ejemplo, la ultima contraseña era "Doggie79" la nueva no debería ser "Doggie80"); y
5) Debe evitar información personal del usuario que alguien podría saber (por ejemplo, cumpleaños, nombres de los niños, etc.).

Es importante notar aquí que estas guías de arriba para contraseñas y configuraciones están basadas por recomendaciones provistas por organizaciones estándar de la industria como NIST, ISO y IEEE. Mientras que contraseñas lo suficientemente complejas son efectivas a sí mismas, estas también pueden ser fácilmente comprometidas por los usuarios finales. Por ejemplo, si las contraseñas son difíciles de recordar, muchos usuarios finales simplemente optan por escribirlas por lo tanto menoscabando su beneficio, esta desventaja debe ser considerada al establecer cualquier régimen de contraseñas.

3.3.2 ***Inicios de Sesión***. Todos los usuarios de la red deben tener un identificador único (ID de usuario o Inicio de sesión) solo para su especifico uso y una adecuada técnica de autenticación debe ser elegida para sustanciar la identidad reclamada por el usuario.

a) IDs de usuarios deben ser capaz de rastrear actividades al individuo responsable. Actividades regulares del usuario no deben ser realizadas desde cuentas con privilegio. En circunstancias especiales donde es clara su necesidad, el uso de un ID compartido por un grupo de usuarios o una función específica de trabajo puede ser usado. IDs genéricos para uso por un individuo puede ser solamente permitido ya sea cuando las funciones accesibles o acciones llevadas a cabo por el ID no necesitan ser rastreados (por ejemplo, acceso solo de lectura), o cuando hay otros controles en sitio (por ejemplo, contraseña para un ID genérico se da solamente a un persona del personal por vez y se registra dicho caso aislado).
b) Donde una autenticación fuerte y verificación de identidad es requerida, métodos de autenticación alternativos a contraseñas, como tarjetas inteligentes, fichas, o formas biométricas son altamente *recomendadas.*

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

3.4 Protección de capas-múltiples

3.4.1 ***Declaración General***. Protección de capas-múltiples debe ser implementada dondequiera y cuando sea posible. Redes con diferentes funciones deben ser implementadas por separado. Por ejemplo, contabilidad de las tragamonedas y redes de tickets deben ser mantenidas por separado y no-enrutables de ser posible. Esta propuesta mantiene aislado cualquier intrusión exitosa. Múltiples capas de seguridad deben ser implementadas para complementar una a otra de modo que si la una falla la otra lo intercepta.

3.5 Encriptación - Transmisión y Almacenamiento

3.5.1 ***Tecnologías de transmisión cifrada***. Todas las redes y protocolos de seguridad deben implementar y soportar encriptación adecuada a los métodos de comunicación para la transmisión de información confidencial o datos/información sensitivos. Note que lo que constituye "confidencial o datos/información sensitiva" puede variar ampliamente. Por lo menos, información personal alta como lo son PINs y Números de Seguro Social serian vistos como confidenciales. La importancia de otros datos pudiese variar como una función de cuan críticos esos datos son para la integridad de la red y/u las necesidades del negocio. El operador de la red debe evaluar el tipo de elemento de datos que la red porta y determinar la sensibilidad relativa de esta información. Esta evaluación servirá entonces como una guía para los tipos de medidas de seguridad que sean apropiados para la red.

3.5.2 ***Métodos de Protección Adicionales***. Los métodos de protección listados a continuación deben también ser considerados y utilizados como técnicamente posibles para protección adicional de la red:

a) IPSec – Un grupo de protocolos de autenticación y encriptación adecuados para todos los tipos de tráfico de protocolos de internet (IP) que son usados para crear Redes Virtuales Privadas (VPNs). IPSec permite que la información confidencial sea enviada segura entre

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

dos estaciones-extremas o red sobre un medio de comunicaciones no-confiable. Esto debe ser considerado como una tecnología para asegurar el Internet y otras comunicaciones IP en la conexión de clientes externos autorizados en locaciones definidas;

b) Capa Segura (SSH) (Secure Shell) – Debe ser implementado solamente para la administración remota de datos/información confidencial en sus sistemas;

c) Capa de Sockets Seguro (SSL) (Secure Sockets Layer) – La especificación de capa de sockets seguro debe ser implementado para proveer acceso seguro a datos/información confidencial en los servidores web. Cuando SSL es usado para proteger información confidencial, debe usarse la versión más actual con un cifrado de 128-bit;

d) Redes Virtuales Privadas (VPNs) (Virtual Private Networks) – Deben ser implementados en ambientes donde la encriptación de dato-enlace-capa no es un solución práctica para mantener y operar. Tecnología VPN usando IPSec o cifrado SSL puede ser implementado independiente de una capa-enlace particular tecnología de comunicaciones (por ejemplo, Alto-Nivel Datos Enlace Control / HDLC, Relay de Cuadro, Fibra Distribuida de Interface de Datos / FDDI, Ethernet, Gigabit Ethernet, Modelo de Trasferencia Asincrónico / ATM, etc.) Como tal, este recurso de buenas prácticas recomienda encarecidamente el uso de tecnología VPN para asegurar las comunicaciones confidenciales;

e) Encriptación Dato-Enlace (simétrico) Data-Link – Debe ser usado en ambientes donde la administración de una Red Virtual Privada no es una implementación de encriptación razonable para mantener y operar, o donde el uso y administración de la tecnología VPN no es justificado;

f) Seguro/Multipropósito Extensión de Email de Internet (S/MIME) – Igual que Pretty Good Privacy (PGP), S/MIME es una mejora a la seguridad basado en estándares para asegurar correo electrónico y adjuntos de mensajes que proporciona una autenticación fuerte mediante firmas digitales, confidencialidad del mensaje, integridad y no-repudiación.

g) Pretty Good Privacy (PGP) – Debe ser utilizado para proteger información sensitiva, transmitida vía correo electrónico, usando un tamaño-llave mínimo de 2048 bits.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Información de la llave pública puede ser mantenida en público o en servidores de llaves PGP internos.

h) Infraestructura de la Lave Publica (PKI) – Recomendada funcionalidad técnica basada en PKI está definida por el estándar X.509 y sus extensiones, en la evolución de definición desarrollada por el Grupo de Trabajo de Ingeniería del Internet (IETF), a través de PKIX Grupo de Trabajo de Desarrollo de Estándares. Este documento provee y define identificación certificada de firmas digitales teniendo integridad, no-repudiación, y autenticación.

3.5.3 Disco (almacenamiento) Encriptación.

a) Dondequiera que información sensitiva es almacenada en disco esta debe utilizar alguna forma de encriptación.

b) Bases de datos que son utilizadas para almacenar información sensitiva o protegida debe ser configurada para habilitar encriptación por defecto. La encriptación de de campos de bases de datos sensitivos es también aceptable otro método es utilizado para prevenir el husmeo (sniffing) de red.

3.5.4 Tecnologías para la Encriptación de Dispositivos de Almacenamiento. Todo dato/información confidencial alojado dispositivos de almacenamiento directamente adjuntos (DAS), y todos dispositivos de almacenamiento portables[3], debe ser cifrado y debe emplear al menos uno o más de los métodos de encriptación anotados a continuación para la protección de datos confidenciales e información protegida:

a) Encriptación de Disco Completo – Encriptado de todos los datos en un disco duro de un dispositivo cliente. Esto incluye el sistema operativo entero, todas las aplicaciones y todo dato/información. Software de encriptación de disco completo contiene componentes que son independientes del sistema operativo y se ejecutan antes de que el sistema operativo sea cargado a sí mismo como la autenticación. El sistema se hace ininteligible y no usable en el caso de un crimen cibernético o terrorismo.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

i. ***Encriptación de Disco Completo debe tener las siguientes funciones:*** Autenticación de Pre-Arranque laptops / PC's de mesa; funciones de encriptación basado en archivos y carpetas incorporado dentro del sistema operativo; soporte de inicio de sesión singular; capacidad de instalación remota; soportar múltiples algoritmos y tener la habilidad de deshabilitar algoritmos soportados y no soportados en caso de conflicto.

b) Encriptación de Archivos (Carpetas) – Provee encriptación para archives o carpetas especificas. Soluciones de encriptación de archivos provee seguridad automática ya que cada capacidad de encriptación de archivo/carpeta nueva debe ser manualmente activada/desactivada.

i. ***Encriptación de archivo (carpeta) debe tener las siguientes funciones:*** Debe ser capaz de soportar todos los estados del sistema operativo, todas las aplicaciones y programas de software relacionados en adiciona los programas de productividad para el estado, habilidad de soportar una multitud de servidor(es) y sistemas de archivos, proveer simples mecanismos de recuperación de llaves perdidas o archivos/carpetas encriptados, integrarse sin problemas con correo electrónico móvil; soportar conceptos de seguridad y métodos de "separación de responsabilidades".

c) Medios de Encriptación de Copia de Respaldo y Archivos – Provee beneficios no solo para proteger los datos almacenados pero también el despojo de copias de seguridad y medios de archivo, mientras los reglamentos divulgados generalmente dictan un periodo de retención par las copias de respaldo y archivo de datos. Sin encriptación, el despoje de los medios es difícil; por lo tanto muchas entidades mantienen copias de respaldo y medios de archivo más tiempo de lo necesario o prudentemente legal. Al borrar la llave de encriptación, el medio se no se puede leer. Con una secuencia de rotación de llaves, un patrón regular de retención y despojo puede ser esforzado automáticamente.

i. ***Medios de Encriptación de Copia de Respaldo y Archivos deben tener las siguientes funciones:*** Integrarse sin problemas en el proceso de respaldo y

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

dispositivos; ofrecer opciones flexibles para la restauración de datos y recuperación de desastres y soportar varios tipos de respaldo usados por el estado.

d) Encriptación de almacenamiento masivo (SAN/NAS) – Provee encriptación para largos volúmenes de datos/información. Dispositivos de almacenamiento masivo se refieren al área de almacenamiento de la red (SAN) y Almacenamiento Adjunto a la Red (NAS) soluciones de administración de datos. Recientemente los límites entre sistemas NAS y SAN se han superpuesto con algunos productos suministrando ambos protocolos a nivel de archivo (NAS) y protocolos de nivel bloque (SAN).

i. ***Encriptación de almacenamiento masivo (SAN/NAS) deben tener las siguientes funciones:*** Soportar encriptación a través del ciclo de vida de todo dato/información ya sea en almacenamiento o en tránsito; métodos de encriptación y des-encriptación deben tener ambas segmentaciones lógicas y físicas, proveer encriptación-des-encriptación eficiente a través de múltiples tipos de almacenamiento masivo incluyendo discos con canales de fibra dentro de un ambiente de red basado en IP.

e) Encriptación de Base de Datos – Implica la encriptación de datos físicos dentro de una base de datos al cifrar la base de datos entera, o funciones de llamado, o procedimientos almacenados y accionantes de la base de datos, o nativamente usando funciones de encriptación del sistema de administración de la base de datos (DBMS) para el encriptado de todo o una parte (columna, línea o nivel de campo). La encriptación de la base de datos puede ser implementada al nivel de aplicación.

i. ***La Encriptación de Base de Datos debe tener las siguientes funciones:*** Soportar encriptación simétrica y asimétrica; habilidad de realizar encriptaciones a nivel de columna/fila vs. Encriptación de la base de datos completa para mayor flexibilidad; soportar múltiples plataformas de bases de datos y sistemas operativos; habilidad de encriptado y des-encriptado al nivel de aplicación u/o campo; soportar la separación de responsabilidades entre el administrador de la base de datos y su administrador “clave”.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

f) Encriptación de Unidades y Dispositivos de Almacenamiento Removibles – Provee encriptación para pequeños dispositivos portables y conjunto de datos existentes. Una unidad flash Bus Serial Universal (USB) comprende una tarjeta de memoria que se conecta al puerto USB de una computadora y funciona como un disco duro portable que no contiene partes en movimiento. Una unidad flash USB es comúnmente conocida como "unidad flash", "unidad thumb", "pen drive", "unidad de llavero", " unidad clave", "llave USB", "cartucho USB", o "llave de memoria".

i. ***Encriptación de Unidades y Dispositivos de Almacenamiento Removibles debe tener las siguientes funciones:*** Unidades USB flash deben tener la capacidad de contraseña/seguridad incorporado dentro del dispositivo. Unidades USB flash y dispositivos de almacenamiento removibles pueden ser comprados con software de encriptación instalado en el hardware del dispositivo, o software de encriptación de archivos puede ser comprado luego del hecho para su instalación.

3.5.5 ***Anchura Mínima de Llaves de Encriptación***. El mínimo ancho (tamaño) de las llaves de encriptación debe ser de 128 bits para algoritmos simétricos y 1024 bits para llaves públicas.

3.5.6 ***Manejo de Llaves de Encriptación***. Debe haber implementado un método seguro para el cambio del conjunto de llaves de encriptación actuales. No es aceptable usar solamente el conjunto de llaves de encriptación actuales para la encriptación del siguiente conjunto. Un ejemplo de un método aceptable para el intercambio de llaves es el uso de técnicas de encriptación de llave pública para transferir el nuevo grupo de llaves.

3.5.7 ***Almacenamiento de Llave de Encriptación***. Debe haber un método seguro en su lugar para el almacenamiento de cualquier llave de encriptación. Las llaves de encriptación no deben ser almacenadas sin estar encriptados a sí mismas.

3.6 Conexiones Externas

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

3.6.1 ***Declaración General***. Conexiones externas a redes operacionales deben ser dirigidas a través se gateways seguras y protegidas por al menos uno de los siguientes métodos de encriptación, como sea aplicable:

a) Seguridad en la Capa de Transporte (TLS) o Capa de Socket Seguro (SSL) debe ser empleado entre el servidor web y el navegador para autenticar el servidor web y, opcionalmente, el navegador del usuario. Las implementaciones de TLS y SSL deben permitir dar soporte la autenticación de cliente usando los servicios provistos por las Autoridades Certificadoras. El uso de SSLv2 y TLSv1.0 son obsoletos al momento de la publicación de este documento.

b) Seguridad IP (IPSec) debe ser utilizado para extender el protocolo de comunicaciones IP, proporcionando confidencialidad de extremo a extremo para los paquetes de datos viajando sobre el internet. El modo apropiado de IPSec debe ser usado acorde con el nivel de seguridad requerido para los datos siendo transmitidos: autenticación e integridad del emisor sin confidencialidad o autenticación e integridad del emisor con confidencialidad.

c) VPNs deben ser usadas para interconectar dos redes que se cruzan y comunican sobre redes inseguras como internet público, estableciendo un enlace seguro, típicamente entre los firewalls, utilizando protocolo de criptografía de túnel aceptado por la industria como lo es IPSec o L2TP. VPN's son recomendados para uso en accesos remotos.

d) Autenticación Remota de Servicio de Usuario Dial-In (RADIUS) es un protocolo de servidor de cliente/servidor que habilita los servidores de acceso a la red para comunicarse con el servidor central para autenticar y autorizar usuarios remotos acceso a los sistemas o servicios, una fuerte autenticación debe ser usada para sistemas con módems dial-up.

e) Módems Dial-up de estaciones de trabajo deben ser deshabilitados y removidos. El uso de hardware y herramientas de escaneado de inventario para verificar la presencia y configuración de utilidades de marcado (dial) y módems debe ser implementado. Cualquier uso de sistemas de modem dial-up deben ceñirse a las pólizas aceptadas por el operador/parte interesada de la red que pueden incluir:

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

i. Una lista actual completa de todo el personal autorizado con privilegios de acceso modem.

ii. Documentación automática luego de un especificado periodo de inactividad. Parámetros de inactividad deben ser determinados por el operador de la red/partes interesadas en línea con las necesidades operacionales.

iii. El recomendado uso de tokens de seguridad.

iv. Terminación inmediata de privilegios de acceso modem luego de una transferencia de empleo, re- asignación, o terminación.

f) Donde se dicte la sensibilidad de datos, fuerte autenticación, como dispositivos de reto/respuesta, contraseñas de un solo uso, tokens, kerberos, y tarjetas inteligentes deben ser usados una vez que se ha otorgado permiso para conectar.

g) Conexiones externas deben ser removidas prontamente cuando ya no son requeridas. Componentes claves de la red deben ser deshabilitados o removidos para prevenir reconexión inadvertida.

3.7 Programas de Protección para Antivirus y Malware

3.7.1 ***Protección de Antivirus y Malware.*** Donde sea aplicable, programas de antivirus y malware utilizados con propósitos de seguridad de la red deben:

a) Ser mandatorios en todos los sistemas.

b) Ser actualizados automáticamente, o en caso de no ser posible debido a otras limitaciones, ser actualizado regularmente a través de algún medio manual. Si se requieren actualizaciones manuales, su frecuencia debe ser especificada en la Póliza de Seguridad.

c) Incluye ambos, escaneado del sistema de archivos y procesamiento en tiempo real. (Note que el escaneado puede afectar adversamente el rendimiento en tiempo real de la red. De manera que este factor debe ser considerado al seleccionar un enfoque específico.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

d) Idealmente aprovechar soluciones de vendedores múltiples entre el sistema host y servicios Gateway (por ejemplo Gateway de correo electrónico). Esto es consistente con una filosofía de implementación de multicapas.

3.8 Parches y Actualizaciones del Software

3.8.1 ***Declaración General***. Los operadores/partes interesadas de red deben desarrollar e implementar procedimientos escritos que delinean los roles y responsabilidades para la administración de parches y actualizaciones para el software que cubra las siguientes actividades:

a) Los operadores/partes interesadas de red deben monitorear proactivamente y ocuparse de las vulnerabilidades de todos los dispositivos de red (enrutadores, firewalls, conmutadores, servidores, dispositivos de almacenamiento, etc.) asegurando que los parches aplicables son adquiridos, ensayados, e instalados en un tiempo oportuno.

b) Donde sea posible, los parches deben ser instalados y validados en un ambiente de prueba antes de su introducción a un ambiente de producción. Los ensayos ayudaran a exponer impactos perjudiciales a las aplicaciones de software y/o dispositivos de red antes de la implementación en una red en tiempo real.

c) Donde sea posible, la instalación de parches debe ser completada con el uso de herramientas automatizadas como Servicios de Actualización de Servidor Windows (WSUS) o repositorios locales (variantes UNIX). Los estados de los parches desplegados deben ser monitoreados.

d) Donde sea posible, las configuraciones de sistema deben ser respaldados antes de la instalación de los parches.

3.9 Recuperación de Desastres (Lógico)

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

3.9.1 ***Declaración General***. Las redes son vulnerable a una variedad de disrupciones que van desde leves (por ejemplo, corte de energía de corto tiempo, falla de unidad de disco) a severa (por ejemplo, destrucción de equipo, fuego) derivados de una variedad de fuentes como desastres naturales, hackers, virus, etc. Mientras que muchas vulnerabilidades pueden ser minimizadas o eliminadas a través de soluciones técnicas, administración u operacionales como parte de los esfuerzos de administración de operador/partes interesadas de la red, es virtualmente imposible eliminar completamente todos los riesgos. En muchos casos, recursos críticos pueden alojarse fuera del control del operador/parte interesada (como lo son las fuentes de energía eléctrica o telecomunicaciones), y los operadores/partes interesadas de la red pueden ser incapaces de asegurar su disponibilidad. Efectivo planeamiento de contingencia, ejecución, y ensayo son esenciales para mitigar los riesgos del sistema y la indisponibilidad de servicio. La recuperación de desastres esta dirigida para asegurar que todos los datos críticos sean recuperables bajo demanda y que estos puedan ser puestos de regreso a un estado usable tan pronto y eficientemente posible.

3.9.2 ***Planificación de Recuperación de Desastres***. Los componentes del planeamiento de recuperación de desastres y contingencia deben reflejar los siguientes criterios:

a) Continuo análisis de impacto del negocio debe ser completado en un esfuerzo de identificar y priorizar críticos sistemas y componentes IT.
b) Mantenimiento y controles preventivos deben ser implementados para reducir los efectos de disrupción de sistemas e incrementar la disponibilidad del sistema.
c) Minuciosas estrategias de recuperación deben ser implementadas para asegurar que el sistema pueda ser rápidamente y efectivamente recobrable luego de una disrupción. Estas estrategias deben incluir adecuada administración de respaldo, replicaciones y sistemas sobre falla.
d) Un plan de contingencia debe ser desarrollado y adherido y debe contener guía y procedimientos detallados para restaurar sistemas y/o datos dañados.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

e) Ensayos planeados, entrenamiento, planes de ejercicios de contingencia deben ocurrir regularmente en un esfuerzo de exponer brechas en la efectividad de la ejecución del plan y asegurar que el personal este familiar con su ejecución.

f) Planes de contingencia deben ser documentos con vida que son actualizados regularmente para mantenerse actualizado con los cambios y mejoras de los sistemas.

3.10 Prevención y Detección de Intrusos

3.10.1 ***Declaración General***. Detección de intrusos es el proceso de monitorear los eventos ocurriendo en un sistema computarizado o red y analizando estos por señales de posibles incidentes, que son violaciones o amenazas inminentes de violación a la póliza de seguridad de las computadoras, pólizas de uso aceptable, o practicas de seguridad estándar. Prevención de intrusión es el proceso de realizar la detección de la intrusión y tratar de frustrar posibles incidentes.

3.10.2 Un Sistema de Detección de Intrusos (IPS) debe estar integrado en las redes operacionales para monitorear proactivamente todos los dispositivos de la red de intrusión no autorizada, y debe conformar con los siguientes criterios mínimos:

a) Sistemas de Detección de Intrusos deben ser implementados en ambos interno y externo en adición a las soluciones de firewall existentes. Reportes de detección de intrusos deben ser revisados regularmente por el operador/partes interesadas de la red y todos los incidentes deben ser reportados y resueltos de forma oportuna.

b) Con respecto a los servidores, los Sistemas de Detección de Intrusos deben monitorear por cambios no autorizados hechos a archivos (integridad de archivos), especialmente para archivos críticos del sistema.

c) Procedimientos deben ser implementados para proveer la revisión del tráfico de la red. Trafico de la red debe ser revisado por la presencia de anomalías que pueden ser indicativos de ataques o dispositivos configurados incorrectamente.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

d) Sistemas de Prevención de Intrusión deben incluir parámetros de seguridad definidos por usuario que ayudaran a establecer las bases útiles de rendimiento en establecer un apropiado conjunto de pólizas de seguridad.

e) Lenguaje de Descripción de la Vulnerabilidad de Aplicaciones (AVDL) es un estándar propuesto de seguridad de interoperabilidad. AVDL crea una vía uniforme de describir las vulnerabilidades de seguridad de aplicaciones usando el Lenguaje de Marcado Extensible (XML). La tecnología basada en XML permitirá la comunicación entre productos que buscan, bloquean, reparan y reportan huecos de seguridad de las aplicaciones. El uso de AVDL es *recomendado* pero no requerido.

f) Las tecnologías de prevención de intrusión pueden reducir el número de falsas alarmas al enfocarse en un comportamiento heurístico en tiempo real en vez de usar la tecnología de coincidencia de firma para identificar potenciales ataques de red. Tecnologías de prevención de intrusión pueden también prevenir ataques "día – cero" que explota debilidades desconocidas, porque estas responden a un cambio en el estado normal de operación, de cualquier manera, positivos falsos pueden seguir siendo comunes.

g) Sistemas IPS deben ser utilizados en sistemas o dispositivos que no pueden ser parchados propiamente para proveer un nivel apropiado de seguridad para esos sistemas. Dispositivos IPS deben también ser utilizados para proteger sistemas con vulnerabilidades conocidas durante un tiempo extendido requerido para el proceso de administración de parches.

3.10.3 ***Protección de Intrusión***. Todos los servidores deben tener suficiente protección de intrusión física/lógica en contra de acceso no autorizado. Idealmente, debe requerir autoridad del fabricante y operador/parte autorizada de la red, así proporcionando acceso conjuntamente pero no por separado. Mientras que un IDS es capaz de detectar y reportar una intrusión no autorizada, un IPS está diseñado para prevenir acceso no autorizado y rechazar el tráfico de ganar acceso en primer lugar.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

3.11 Escaneando Vulnerabilidades

3.11.1 ***Declaración General***. Donde sea práctico, el escaneado de red y host, debe ser usado para hacer pruebas para vulnerabilidades de dispositivos de red interna, aplicaciones y defensas del perímetro de red, así mismo apegarse a la póliza de seguridad y estándares.

3.11.2 ***Herramientas para el Escaneado de Vulnerabilidades***. Donde sea técnicamente posible, una herramienta de escaneado de vulnerabilidades automático debe ser usada para escanear la red por "servicios vulnerables" conocidos (por ejemplo, un sistema que permite anónimamente el Protocolo de Transferencia de Archivos (FTP), retransmisión de correo enviado, etc.). se debe notar comoquiera que algunas de las potenciales vulnerabilidades identificadas por la herramienta de escaneado automático pueda que no representen vulnerabilidades reales en el contexto del ambiente del sistema. Por ejemplo, algunas de estas herramientas de escaneado clasifican potencial vulnerabilidades sin considerar el ambiente del sitio y requerimientos. Algunas de las vulnerabilidades marcadas por el software de escaneado automático pudieran ser en realidad vulnerabilidades para un sitio en particular pero tal vez están configurados de esa manera porque lo requiere el ambiente particular de la red.

3.11.3 ***Escáner de Vulnerabilidad***. Es recomendable que los escáneres de vulnerabilidad tengan la habilidad de manejar por lo menos las siguientes tareas:

a) Sistemas de inventario y servicios incluyendo parches aplicados.
b) Identificar huecos de seguridad al confirmar las vulnerabilidades.
c) Proveer reportes comprensivos y gráficos para la toma de decisión efectiva y mejora de seguridad.
d) Definir y hacer cumplir las pólizas de seguridad validas cuando son usadas durante la instalación de seguridad del dispositivo y certificación.
e) Usar cautela en el escaneo para verificar la operación propia de dispositivos IDS/IPS.
f) Idealmente el escaneado de vulnerabilidad debe incluir ambos escaneados la red y nivel de aplicación.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Cualquiera de estos puede ser reemplazado por un proceso manual cuando se necesite/desee. Esto puede ser deseable especialmente para el punto b) como herramienta automática para verificar vulnerabilidades que puedan causar interrupciones.

3.12 Registro

3.12.1 Registro de Seguridad.

a) Capacidades de registro deben ser habilitadas en dispositivos donde se soporte.
b) Los registros deben ser revisados con una frecuencia determinada y documentado por el operador/parte interesada de la red. Esto incluye la verificación manual de reportes automatizados de herramientas de análisis.
c) Los reportes deben ser mantenidos localmente y ser reflejados periódicamente a un servidor central para prevenir manipulación de los datos al nivel del sistema.
d) Todos los dispositivos de red deben aprovechar los servidores de protocolo de tiempo de red para estandarizar las estampas de tiempo para los datos de reporte para asegurar que una propia línea de tiempo sea recreada en case de un incidente.

3.12.2 Sincronización de Reloj. Para facilitar los reportes, los relojes de todos sistemas procesando información relevante dentro de una organización o dominio de seguridad deben estar sincronizados con lo acordado antes y una fuente exacta de tiempo.

3.13 Acceso Remoto

3.13.1 Declaración General. Acceso remoto es definido como cualquier acceso al sistema fuera de la red "confiable". El acceso remoto donde sea permitido, debe autenticar todos los sistemas computacionales basados en las configuraciones autorizadas de la red o aplicación firewall que

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

establece la conexión con la red. La seguridad de acceso remoto será revisado en bases de caso por caso en conjunto con la tecnología actual y aprobado por el operador/parte interesada de la red.

3.13.2 ***Requerimientos de Acceso Remoto.*** Si se soporta, una red puede utilizar acceso remoto controlado por contraseña siempre y cuando se cumplan los siguientes requisitos:

a) Una reporte actividad de usuario de acceso remoto debe ser mantenida como se describe a continuación;
b) No funcionalidad autorizada debe ser permitida de administración de usuario remoto (añadir usuarios, cambio de permisos, etc.)
c) No acceso autorizado debe ser permitido a la base de datos otro que la recuperación de datos usando funciones existentes;
d) Un filtro de red (firewall) debe ser instalado para proteger el acceso.

NOTA: *GLI reconoce que los fabricantes de sistemas pudieren, como sea necesario, acceder remotamente a la red y sus componentes asociados con el propósito de soporte al usuario y del producto, si es permitido.*

3.13.3 ***Reportes de Auditoria de Acceso Remoto.*** El servidor de red debe mantener un reporte de actividad ya sea automático o tener la habilidad para manualmente ingresar al reporte que muestra toda la información de acceso remoto. Reportes de acceso remoto deben como mínimo incluir lo siguiente:

a) Nombre de inicio de inicio de sesión del usuario;
b) Hora y fecha en que la conexión fue hecha.
c) Duración de la conexión; y
d) Actividad mientras conectada, incluyendo las áreas específicas accedidas y cambios hechos.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

CAPITULO 4

4.0 REDES INALÁMBRICAS

4.1 Estándares de la Industria

4.1.1 Estándares de la Industria para Redes Inalámbricas. La mayoría de estándares inalámbricos hoy en uso evolucionaron del trabajo del Instituto de Ingenieros de Electricidad y Electrónicos (IEEE). Este cuerpo desarrolla estándares para un amplio rango de tecnologías incluyendo inalámbricas. El IEEE desarrollo el primer estándar inalámbrico LAN, 802.11, en el pasado 1997. Muchas iteraciones de este estándar inalámbrico básico han sido promulgadas desde ese tiempo.

4.2 Consideraciones Únicas

4.2.1 Declaración General. La interface inalámbrica define el contorno de comunicación entre dos entidades, como una parte de software, un dispositivo hardware, o el usuario final. Esto también puede proveer un medio de traducción entre las entidades que no hablan el mismo idioma. Esta sección lidia con interfaces de software que existen entre separados componentes de hardware y software que componen el sistema inalámbrico y quienes proveen un mecanismo programático de manera que esos componentes puedan comunicarse.

4.2.2 Protocolo de Comunicación. Cada componente de una red inalámbrica debe funcionar como indicado por el protocolo de comunicaciones implementado. Todas las comunicaciones entre el servidor(es) y el cliente móvil deben usar autenticación apropiada y protocolos criptográficos para proveer autenticación mutua del dispositivo móvil y el servidor, asegurando la integridad de los datos comunicados, y para la confidencialidad, encriptado de los datos comunicados. GLI recomienda encarecidamente el uso del comercialmente disponible 802.1(x)

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

dispositivos con protocolo-compatible en conjunto con otros componentes concisos de seguridad aplicables. Cualquier implementación alternativa será revisada en bases de caso por caso con la aprobación del operador/parte interesada de la red.

4.2.3 Servidor Inalámbrico Usado con Otros Sistemas. En el caso de que el servidor inalámbrico es usado en conjunto con otros sistemas; (por ejemplo, Sistemas de Monitoreo y Control En-Línea, Sistemas de Validación de Tickets, Sistemas Progresivos, etc.) incluyendo acceso remoto, todas las comunicaciones deben pasar por al menos un nivel de aplicación del firewall aprobado, y no debe tener la facilidad de permitir una rute de red alterna a no ser que la ruta alterna se conforme con los requerimientos de este documento y tenga seguridad independiente (por ejemplo, las llaves no son las mismas como en otras redes). Una opción para la autenticación de red es IEEE 802.1X. Como un estándar abierto con soporte para múltiples protocolos de autenticación, 802.1X es suficientemente flexible para soportar todo desde certificados digitales a autenticación de nombre de usuario/contraseña, y plataformas desde el nivel-bajo dispositivos PDA y teléfonos móviles hasta computadores de escritorio y sistemas operativos de servidores.

NOTA: *Cada red revisada por el laboratorio de pruebas independiente será examinada a fondo para asegurar que el campo propuesto de configuración es seguro. El laboratorio de pruebas independiente puede proveer recomendaciones de seguridad adicionales y proveer entrenamiento en el sitio al operador/partes interesadas de la red, si se requiere.*

4.2.4 Seguridad Física de Red Inalámbrica. Una red inalámbrica se debe ajustar a los siguientes requisitos mínimos:

a) Puntos de Acceso Inalámbrico (WAP's) deben estar físicamente localizados de manera que estos no sean fácilmente accesibles al público general;
b) Si el punto anterior no es posible, todos las salidas Ethernet deben estar deshabilitados para reducir el riesgo de intrusión de red;

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

c) La red inalámbrica debe estar preferiblemente designada a ser una red independiente (separada) de acuerdo con múltiples técnicas de capas antes discutidos;

d) La red debe apoyar el monitoreo para evidencia de entradas no autorizadas. Si la entrada ha sido detectada, la red debe imponer controles apropiados para bloquear o deshabilitar los puntos de entrada sospechados, si se es posible, y notificar al operador/parte interesada de la red; y

e) La red debe retener evidencia de cualquier manipulación física de los componentes de hardware.

4.2.5 ***Software de Seguridad de Redes Inalámbricas.*** Una red inalámbrica debe:

a) Ser diseñada o programada de manera que esta se comunique solo con clientes/dispositivos inalámbricos autorizados. El software transferido entre el servidor y el cliente/dispositivo debe ser implementado usando un método que asegure los enlaces del cliente/dispositivo para el servidor, de manera que el software sea usado por clientes/dispositivos autorizados. En general, se usan certificados, llaves, o semillas, estos deben estar codificados, y no deben cambiar automáticamente, en un tiempo como una función del enlace de comunicación. Cada método debe ser revisado por el operador/parte interesada de la red y el laboratorio de pruebas independiente en bases de caso por caso;

b) Emplear encriptación y fuerte autenticación de usuario, con una recomendación de al menos dos métodos de validación previa a la apertura de una sesión inalámbrica. Métodos aceptables incluyen: Nombre de usuario y contraseña, un token físico, tarjeta de identificación inteligente, etc.;

c) Realizar autenticación mutua para asegurar que los clientes solo se comunican con una red valida. Un ejemplo de este tipo de autenticación es el uso de certificados digitales. Luego de unirse a la red, el cliente/dispositivo es presentado con el certificado digital del lado del servidor. Si el cliente/dispositivo confía en el certificado, el proceso de autenticación continua. Si el certificado no es confiable, el proceso terminas;

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

d) Validar los clientes/dispositivos en intervalos de tiempo pre definidos con por lo menos un método de autenticación como se describe antes. Este intervalo de tiempo debe ser configurable basado en los requerimientos del operador/parte interesada de la red;

e) Mantener una lista (base de datos) de clientes/dispositivos autorizados, con los cuales esta puede comunicarse. La lista debe incluir el nombre del cliente/dispositivo, un identificador único de cliente/dispositivo y el correspondiente identificador de hardware (MAC); GLI recomienda implementar la filtración MAC (Control de Acceso de Media) para retrasar a usuarios no autorizados en obtener acceso a la red inalámbrica;

f) Instalar y mantener una con estado independiente (por ejemplo, basado en una tabla de estado) inspección de paquetes del firewall, que puede aislar los puntos de acceso desde otros componentes de red que el casino a desplegado;

g) Ofuscar el Grupo de Identificador de Servicio (SSID) de manera que a la red que se está conectado no es inmediatamente aparente. Esconder el SSID solamente retrasa su descubrimiento;

h) Serrar sesiones activas si la autenticación de usuario a excedido el numero de intentos fallidos; el numero de intentos fallidos debe ser configurable basado en los requerimientos del operador/parte interesada de la red;

i) Proveer un reporte imprimible de los fallidos intentos de acceso a la red, incluyendo la estampa de hora y fecha, el nombre del dispositivo, y el identificador del hardware de todos los dispositivos pidiendo el accesos a la red; y

j) GLI *recomienda* el uso de fuerte autenticación de usuario, autorización y encriptación, que validara al usuario en contra de una base de datos segura. Las comunicaciones entre la red y el dispositivo cliente deben usar protocolos designados para asegurar, autenticar y encriptación de redes inalámbricas. Un ejemplo de protocolo apropiado es IEEE 802.1x. este provee la estructura requerida y permite el uso de métodos de alto-nivel de autenticación como aquellos métodos listados en la tabla a continuación.

802.1x MÉTODOS RECOMENDADOS DE AUTENTICACIÓN		
MÉTODO DE AUTENTICACIÓN	ACRÓNIMO	AUTENTICADO EN CONTRA DE
Protocolo de Autenticación Protegida Extendida	PEAP	LDAP, RADIUS, Kerberos o Servidor Microsoft de Directorio Activo, como también bases de datos alojados en un controlador

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Protocolo de Autenticación Entendible-Seguridad de la Capa de Transporte	EAP-TLS	Gateway seguro.
Protocolo de Autenticación Entendible-Seguridad de la Capa de Transporte por Túnel	EAP-TTLS	
Red Virtual Privada con L2TP/IPSEC	VPN	
Protocolo de Túnel de Punto a Punto	PPTP	
Capa de Sockets Seguro	SSL	

Tabla 1: Métodos de autenticación recomendados para uso con 802.1x

k) A pesar que un intruso puede monitorear el enlace de comunicaciones por aire, los datos dentro del túnel encriptado es prevenido de ser interceptado al implementar uno o más de los métodos listados en la tabla de arriba.

l) No se es recomendado usar un protocolo de autenticación extensible sin-túnel (EAP) métodos listados a continuación, por que los enlaces de dato inalámbricos pudieran ser comprometidos.

802.1X MÉTODOS DE AUTENTICACIÓN NO-RECOMENDADOS	
MÉTODO DE AUTENTICACIÓN	ACRÓNIMO
Protocolo de Autenticación Entendible	EAP
Protocolo de Autenticación Entendible Resumen de Mensaje 5	EAP-MD5
Protocolo de Autenticación Entendible Liviano	LEAP

Tabla 2: Métodos de autenticación no recomendados para uso con 802.1x

4.2.6 ***<u>Fallas de Componente.</u>*** Las redes inalámbricas deben tener suficiente redundancia y modularidad para acomodar la falla de un componente para prevenir la interrupción de operaciones inalámbricas. En adición, debe haber copias de redundancia de cada reporte de auditoría y sistema de base de datos donde sea aplicable, en el servidor inalámbrico con soporte abierto para respaldos y restauraciones. Esto incluye una red inalámbrica que tiene soporte para fallas sobre redundancia. Un esquema de implementación de respaldo debe ocurrir en

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

cumplimiento con la Póliza de Recuperación de Desastre, a pesar que todos los métodos serán revisados en bases de caso por caso por el laboratorio de pruebas independiente.

4.2.7 ***Requerimientos de Recuperación.*** En el caso de una falla catastrófica donde la red inalámbrica no pueda ser restaurada de ninguna otra manera, debe ser posible recargar el sistema desde el último punto de restauración viable y recuperar completamente los contenidos de ese respaldo, es recomendado de que consista de al menos la siguiente información mínima, como sea aplicable:

a) Eventos Significantes;
b) Información de Auditoria; y
c) Información específica del sitio como los valores únicos de configuración, seguridad de cuentas, etc.

4.2.8 ***Comunicaciones y Protocolos Inalámbricos.*** Cuando sea apropiado, el estándar IEEE 802.1x debe ser usado con estándares de redes inalámbricas: IEEE 802.1x (Red de Área Local Inalámbrica (WLAN)), IEEE 802.15 (Red de Área Personal Inalámbrica (WPAN)), IEEE 802.16 (Red de Área Metropolitana Inalámbrica (WMAN)).

a) Seguridad es dirigida en la capa de transmisión con el borrador del estándar 802.11i y en la capa de aplicaciones IP con estándares y pólizas basadas en autenticación y control de acceso.
    i. El algoritmo de Privacidad Equivalente al Cableado (WEP), que es parte del estándar 802.11, debe ser considerado comprometido y no confiable;
    ii. El estándar de Acceso Protegido WiFi (WPA2) y Protocolo de Autenticación Extensible (PEAP) con el IEEE 802.1x estándares de Autenticación de Puertos de Red proveen seguridad mejorada.
    iii. WPA2 permite generado automática de claves por usuario y por sesión mediante 802.1x. Además, las calves se pueden regenerar (volver a generar) periódicamente para incrementar la seguridad.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

iv. Clave Pre-Compartida (WPA-PSK) es susceptible a "ataques de fuerza bruta" (ataques afirmados sobre la repetición). Si esto es usado, el uso de una contraseña muy fuerte es también requerida. GLI *recomienda* el uso de contraseñas generadas aleatoriamente más largo de 16 caracteres conteniendo todo lo siguiente:

- Mayúsculas
- Minúsculas
- Dígitos 0-9
- Símbolos.

v. El mantenimiento de una red inalámbrica segura es un proceso continuo que requiere mayor esfuerzo que el requerido para otras redes y sistemas. Por lo tanto, es importante que los operadores/partes interesadas de la red evalúen los riesgos más frecuentes y pongan a prueba y evalúen los sistemas de control de seguridad cuando las se despliegan tecnologías inalámbricas.

b) WLAN Seguridad del Dispositivo de Punto de Acceso Inalámbrico

i. El Identificador de Grupo de Servicio (SSID) debe ser cambiado de los valores de configuración predeterminados de fábrica y limitar su información de identificación.

ii. La función de difundir el SSID puede ser deshabilitada, requieren que clientes/dispositivos inalámbricos sean pre-configurados para un punto de acceso específico, y cause demoras para usuarios no autorizados.

iii. La administración de contraseñas de acceso puede ser cambiado de su configuración predeterminada y las llaves criptográficas deben ser cambiadas de su configuración predeterminada de fabrica. Las llaves criptográficas deben ser cambiadas con frecuencia.

iv. Dispositivos de punto de acceso deben ser administrados por vía de las herramientas de administración de red usando SNMPv3 o mayor. Si la administración de red no es realizada por el operador/parte interesada de la red, SNMP debe ser deshabilitado.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

v. Dispositivos de Punto de Acceso que operan con un controlador central son recomendados y deben ser deshabilitados durante fuera-de-horas, o cuando no están en uso.

vi. Puntos de Acceso que están conectados al internet por cualquier medio deben tener su tráfico usando una LAN Virtual (VLAN) y/o Traductor de Direcciones de Red (NAT). Las VLAN's están cubiertas por IEEE 802.1Q. El uso de VPN debe ser empleado cuando se acecen recursos internos.

vii. La intensidad de la señal (relación de señal-ruido) de un Punto de Acceso Inalámbrico debe ser auditado y reducido para abarcar solamente aéreas deseadas.

viii. Una lista de Puntos de Acceso Inalámbricos autorizados debe ser mantenidos por el operador de la red. El operador de la red debe escanear la red regularmente por puntos de acceso no autorizado transmitiendo dentro de su perímetro de red definido. Estos puntos de acceso pueden servir como puntos de entrada no protegidos dentro de la red.

ix. Una Lista de Puntos de Acceso autorizado debe ser mantenida por el operador/parte interesada de la red. El operador/parte interesada de la red debe escanear con regularidad por puntos de acceso no autorizados transmitiendo dentro de su perímetro de red definido. Estos puntos de acceso pueden servir como puntos de entrada no protegidos dentro de la red.

c) Dispositivos de Área Personal de Red Inalámbrica (WPAN) usados para acceder a la red, acceso a internet basado-en-red interna, y aplicaciones de software deben:

i. Ser requeridas a acogerse al mismo rango de requerimientos de seguridad como los dispositivos cliente WLAN.

ii. Requiere PIN para entrar u otra autenticación.

iii. Invocar un enlace de encriptación para todas las conexiones y retransmitir las transmisiones.

iv. Estar establecido al nivel más bajo energía suficiente necesario para mantener la transmisión localizada al área inmediata.

v. Requiera dispositivo de contraseñas fuerte como para prevenir el uso no autorizado de dichos dispositivos.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

vi. Usar encriptación al nivel-de-aplicación, tecnologías VPN, y autenticación.

vii. Estar apagados cuando no están en uso.

d) La conectividad de Redes Inalámbricas de Área Metropolitana (WMAN) usadas para interconectar edificios debe usar tecnologías VPN y las transmisiones deben ser encriptados.

e) Tecnología Firewall debe ser implementada a todas las aplicaciones Gateway inalámbricas. Esto es adicional al nivel de seguridad que reducirá acceso no autorizado a redes operacionales.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

CAPITULO 5

5.0 INGENIERÍA SOCIAL Y EDUCACIÓN

5.1 Declaración General

5.1.1 ***Declaración General.*** Ataques de Ingeniería Social incluyen intrusiones a una red no-técnicas usando información obtenida a través de la interacción humana y basada en trucos para victimizar a un individuo que no es familiar con las tecnologías y protocolos emergentes. Los operadores/partes interesadas de la red deben establecer pólizas e implementar los programas de entrenamiento necesarios para atender este tipo de ataques.

5.2 Personificación de Vendedores

a) Los atacantes hacen llamadas a empleados internos personificando a vendedores de hardware, software, o servicios en un esfuerzo de reunir información pertinente a los sistemas internos. Información valorable puede incluir contraseñas o modelos de dispositivos de red.

b) Los empleados deben ser educados de que puede ser considerada información sensitiva y a quien deben dirigir este tipo de consultas dentro de los operadores/partes interesadas de la red.

5.3 Información Disponible Públicamente

a) Una revisión de la información disponible públicamente en relación a las redes operacionales debe ser completado con rutina. Cuando sea posible, este tipo de información debe ser mantenido fuera del conocimiento público.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

b) Dicha información debe incluir, pero no se limita a: nombre de empleados, títulos, números de teléfono, y direcciones de correo electrónico. Información como esta podría ser de gran uso al hacker de una red.

5.4 Seguridad de los Mensajes de Voz

a) Con nada más que un número de teléfono, un hacker puede acezar a información operacional sensitiva que ha sido grabada en mensajes de voz, en cuentas de mensaje de voz con contraseñas débiles.

b) Una póliza para contraseñas de correo de voz relacionado con el largo y complexidad debe ser adoptado y en forzado por el operador/parte interesada de la red.

5.5 Correo Electrónico Dirigido "Phishing"

a) Correo electrónicos enviados a individuos y grupos dentro de la red de operadores/partes interesadas en un esfuerzo de tentar al usuario a revelar información sensitiva.

b) Dispositivos Firewall para correo no deseado deben ser integrados dentro de la red por el operador/partes interesadas de la red para mitigar les ocurrencias de correos no deseados "phishing" siendo entregados a usuarios internos y externos.

c) La combinación de intentos de Phishing estándares con técnicas de Ingeniería Social ("Spear Phishing").

d) El personal debe ser educado sobre como reconocer posibles correos electrónicos peligrosos.

5.6 Eliminación de Documentos Sensitivos

a) Los documentos conteniendo información sensitiva relacionada con la infraestructura de la red deben ser eliminados cuando ya no sean necesarios.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

b) Documentos de papel y medios como CD o DVD deben ser cortados antes de dejar el establecimiento.

c) Discos duros dispositivos de almacenamiento de disco en computadoras y otro equipo electrónico como fotocopiadoras deben ser limpiados de los datos almacenados al final de su ciclo de vida y antes de ser removidos para prevenir acceso a la información segura. Cualquier regulación y requerimiento para archivar datos debe ser observado.

Nota Especial: *La eliminación y/o destrucción de la documentación e información pudiera ser regulada en una jurisdicción en particular. Cualquier manipulación de la documentación sensitiva o información debe cumplir por completo con las prácticas regulatorias locales. Estas prácticas deben estar documentadas en la póliza de seguridad.*

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

CAPITULO 6

6.0 RECURSOS DE CÓMPUTO EN LA NUBE

6.1 Declaración General

6.1.1 Este documento usara la definición de computo en la nube como se publica en la publicación especial NIST 800-145: *"Computo en la nube es un modelo que permite extendido, conveniente, acceso a la red por demanda a un grupo de recursos computacionales configurable (por ejemplo, redes, servidores, almacenamiento, aplicaciones, y servicios) que pueden ser rápidamente provisionados y lanzados con mínimo esfuerzo de administración o interacción del proveedor de servicio. Este modelo de nube está compuesto de cinco características esenciales, tres modelos de servicio, y cuatro modelos de implementación."*

Adicionalmente los términos Consumidor(es), Cliente(s), y Proveedor(es) seguirán las definiciones de la misma fuente.

6.2 Consideraciones Generales

6.2.1 ***Introducción.*** En diversos grados, el mover a una solución de nube desde un modelo cliente-servidor más convencional resulta un cambio potencial en el control del ambiente operativo. En la mayoría de casos, esto es intencional y se considera parte de la meta de subcontratación. La utilización recursos computacionales de la nube puede proporcionar una mayor disponibilidad de recursos mejorando las operaciones de monitoreo y funciones mejoradas de respaldo y recuperación. Mientras que el control físico directo de los recursos de red es subcontratado en un ambiente de computación de nube, el uso de centros da datos seguro localizados discretamente proveen latentemente un nivel similar de seguridad física que los centros de datos local; si bien estos son un poco diferentes en cierta manera, en los ambientes

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

virtuales de nube, la seguridad puede ser mayormente mejorada por la habilidad de "rodar" o trasferir los fácilmente datos a otro centro de datos en el caso de impedimento de desastres naturales u otros potenciales escenarios de falla. Mientras que el uso del cómputo en la nube provee en general una mejora a la seguridad de los datos al permitir la habilidad de ser mas ágil con respecto al monitoreo en general, resguardo, recuperación y salud en general la salud de la actividad del sistema.

6.2.2 ***Verificación de autenticidad.*** La identidad de todas las partes no puede ser tomada no puede ser tomada de un valor frontal. Un mecanismo de verificación de identidad como los son los certificados debe ser empleado y verificado.

6.2.3 ***Acuerdos de servicio****:* Como partes de lo que sería la infraestructura local y están manejadas por terceras partes, los acuerdos de nivel de servicio deben ser detallados y ser capaz de cumplir con lo establecido con la póliza de seguridad local.

6.2.4 ***Seguridad Física.*** El proveedor de la nube debe probar que su seguridad física es certificada, verificable y auditable en relación a un estándar (por ejemplo, ISO27001).

6.2.5 ***Nubes Privadas En-Sitio***. Nubes privadas en-sitio son entornos de nube que están totalmente localizados en las instalaciones del consumidor.

6.2.6 ***Seguridad de Nubes Privadas En-Sitio.*** La seguridad de la nube privada en-sitio es efectivamente la misma que las recomendaciones establecidas en las secciones anteriores de este documento.

6.2.7 ***Nube Privada Fuera-de sitio***. Una red privada fuera de sitio puede ser asegurada de la misma manera que una nube privada en sitio. No deben hacerse hipótesis acerca del nivel de protección dado por el proveedor.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

6.2.8 ***Nube Pública***. En una nube publica, la habilidad de construir un túnel no debe existir, todo tráfico desde y hacia su aplicación podría ser considerado datos sensitivos no-confiable y tendrán que ser encriptados por la aplicación.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

APÉNDICE

LISTA DE FIGURAS

Figura 1 – Ejemplo de la Topología de una Red con Cableado

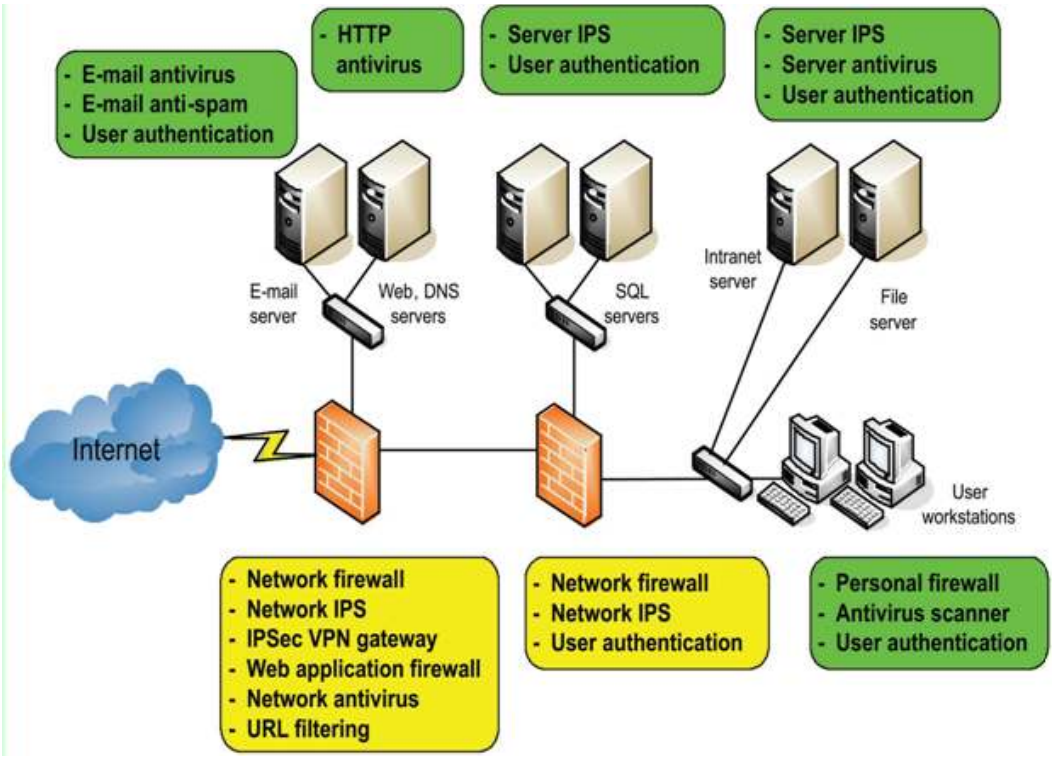
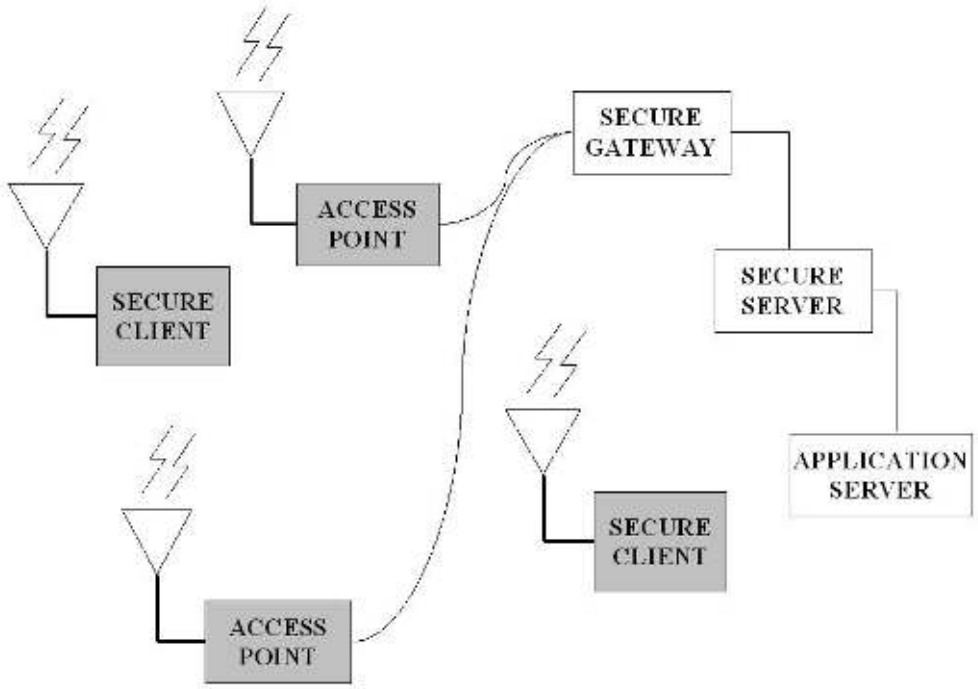


Figure 1 – Topología de una Red Cableada, también muestra posibles esquemas de seguridad.

Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.

Figura 2 – Topología para una Red Inalámbrica



Derechos de Autor © 2013 Gaming Laboratories International, LLC Todos los Derechos Reservados.