ESTÁNDAR DE BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA

CAPITULO 1

1. VISIÓN GENERAL

1.1. Introducción

Una red es una serie de puntos o nodos interconectados por caminos de comunicación. Las redes pueden ser definidas por su topología o configuraciones generales, también pueden caracterizarse en términos de distancia espacial como redes de área local (LAN), y redes de área amplia (WAN). Otras características pueden ser contempladas haciendo referencia al tipo de tecnología para la transmisión de datos en uso; ya sea que este lleve audio, 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.

1.2. Principios de Diseño de Seguridad de Redes.

Se definen los siguientes principios de seguridad con los que deberán contar las redes de datos y comunicación que se implementen en la operatoria de salas de juego:

a) Integridad, significa que las medidas de seguridad sean preservadoras. Estas deben proteger la confidencialidad y sensibilidad de los datos de una forma consistente todo el tiempo y no deben corromper los mismos.
b) Disponibilidad, significa que las medidas de seguridad estén disponibles continuamente, al igual que los sistemas y datos que se están protegiendo.
c) Protección adecuada, significa que lo que se está protegiendo, lo sea a un nivel proporcional con su valor. Los elementos informáticos deben ser protegidos sólo hasta que estos pierdan su valor.
d) Efectividad, significa que cualquier control que esté implementando sea efectivo, asegurando la red y las partes de sus componentes. Estos también deben ser eficientes, de fácil uso y apropiados para el tamaño y tipo deorganización.
e) Protección de profundidad, se debe suponer que un intruso intentará utilizar cualquier medio de penetración disponible. Esto no implica necesariamente los medios más obvios, ni es necesariamente contra el cual se ha instalado la defensa más sólida
f) Debida diligencia, asegurar la seguridad de la red es un proceso continuo y en evolución. La red debe ser monitoreada y manejada perpetuamente para asegurar su seguridad.

1.3. Definiciones Claves de Seguridad de Red

1.3.1. Objetivos de la Seguridad de Red

La seguridad de la red equivale a la protección de redes y sus servicios, dicha seguridad deberá contemplar modificaciones no autorizadas, destrucción, divulgación, la garantía que la red realiza sus funciones críticas correctamente y que todo el software en la red es auténtico y original del fabricante. La seguridad de la red también ayuda a asegurar la integridad de los datos que atraviesan por la misma.

1.3.2. Definiciones.

Estándar de Encriptación Avanzado (AES)	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.

Auditoría de Datos	Registro cronológico de las actividades del sistema que permiten la reconstrucción y examinación de la secuencia de eventos y cambios en un evento.
Auditoría de Rastreos	Registro que muestra quien ha accedido a un sistema de tecnología de información y qué operaciones ha realizado el usuario durante un periodo determinado
Autenticación	Verificar la identidad de un usuario, proceso, paquete de software o dispositivo, a menudo como un requisito previo para permitir el acceso a los recursos en un sistema de información
Respaldo	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, incluyendo operaciones informáticas, posibilidad de una locación alternativa, en caso de emergencia, fallas del sistema o desastres.
Integridad de Datos	Propiedad de que los datos son precisos, consistentes y que no han sido alterados de manera no autorizada. La integridad de los datos cubre los datos almacenados durante el 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)	Plan escrito para procesar aplicaciones críticas y prevenir la pérdida de datos en caso de un evento mayor de falla del hardware o software o destrucción de las instalaciones.
Clave Criptográfica	Clave se ha cifrado 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.

Red Encriptada	Red en la que los mensajes se codifican para evitar que personas no autorizadas los lean.
Encriptación	Conversión de datos en una forma llamada texto cifrado (ciphertext), el cual no puede ser comprendido fácilmente por personas no autorizadas.
Firewall	Mecanismo o dispositivo que limita el acceso entre Redes de acuerdo con la política de seguridad local.
Honeypot	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 que no tiene usuarios autorizados, exceptos administradores.
Incidente	Violación o amenaza inminente de transgresión de las Políticas de seguridad informáticas, o prácticas de seguridad informática estándar. Cualquier ocurrencia que actual o potencialmente pone en peligro la confidencialidad, integridad, o disponibilidad de un sistema informático o la información de los procesos, almacenamiento, o tráfico del sistema, o que constituye una violación o amenaza inminente de violación de las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptables.
Plan de Respuesta a Incidentes	Documentación de un conjunto predeterminado de instrucciones o procedimientos cuando se encuentra un ciberataque malicioso contra los sistemas de TI de una 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 antes que ésta alcance sus objetivos.

Dirección IP	Número único para una computadora que es usado para determinar dónde deben entregarse los mensajes que son transmitidos sobre cualquier red.
Seguridad IP (IPSec)	Conjunto de protocolos para asegurar las comunicaciones del protocolo de internet (IP) autenticando y encriptando cada paquete IP de un flujo de datos. IPsec también incluye protocolos para establecer autenticación 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), solicitud de Comentarios (RFC) 2411, protocolo que proporción capacidad de seguridad en la capa de comunicaciones del protocolo de internet (IP). El protocolo de administración de claves 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 caracterizarán la VPN. El protocolo de administración de llaves más usado es el protocolo de Intercambio de Llaves de Internet (IKE).
KERBEROS	Es un protocolo de autenticación de red diseñado para proporcionar una fuerte autenticación para aplicaciones cliente/servidor usando criptografía de clave simétrica.
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 de Autenticación de mensajes (MAC)	Es una suma de verificación (checksum) criptográfica para detectar modificaciones de datos accidentales e intencionadas de los datos.
No-repudiación	Certeza de que el emisor de la información es provisto con una prueba de entrega y el receptor es provista con prueba de la identidad del emisor, de manera que ninguno pueda luego negar el haber procesado la información.

Contraseña	Es un código secreto, o una cadena de caracteres, letras números (letras, números, y otros símbolos) usados para autenticar una identidad o para verificar la autorización de acceso.
Número de Identificación	Es un código alfanumérico o clave usado para autenticar una identidad.
Phishing	Es engañar a individuos a revelar información personal sensible mediante métodos informáticos engañosos.
Política para la Seguridad	Es un documento que delinea la gestión de la seguridad y estructura y asigna claramente las responsabilidades de seguridad y sienta las bases necesarias para medir de manera confiable el progreso y cumplimiento.
Puerto	Es un punto físico de entrada o salida de un modulo criptográfico que provee acceso al módulo para señales físicas representado por el flujo de información lógica (puertos separados físicamente no comparten el mismo pin físico o cableado).
Llave Privada	Es la parte secreta de un par de llaves asimétricas que normalmente se utiliza para firmar o descifrar datos digitalmente. El cifrado de clave Asimétrica utiliza diferentes claves para cifrar y para descifrar. Estas llaves están matemáticamente relacionadas y forman un par de llaves.
Proxy	Un proxy es una aplicación intermedia que se usa entre el cliente y el servidor. El proxy acepta ciertos tipos de trafico entrante o saliente de una red, los procesa y los renvía. Esto cierra efectivamente la ruta directa entre las redes internas y externas. Dificultando para un atacante obtener direcciones internas y otros detalles de la red interna de la organización. Servidores proxy están disponibles para servicios de internet común.
Llave Pública	Es la parte pública de un par de llaves asimétricas que normalmente se utiliza para verificar firmas o encriptación de datos típicamente usado para verificar firmas o encriptación.
Acceso Remoto	Acceso por usuarios (o sistemas de información) que se comunican externamente a un perímetro de seguridad del sistema de información.
Riesgo	Es la probabilidad que una amenaza tenga éxito en su ataque contra la red.
Protocolo de Comunicación Seguro	Un protocolo de comunicación que provee apropiada confidencialidad, autenticación y protección de integridad del contenido.
Ingeniería Social	Es una estratagema o engaño que alguien utiliza para hacer revelar información (por ejemplo una clave) que puede ser usado para atacar los sistemas o redes.

Amenaza	Es cualquier circunstancia o evento con el potencial de afectar adversamente 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 denegación de servicio. Además, el potencial de una fuente de amenaza para explotar con éxito una vulnerabilidad particular del sistema de información.
Acceso No-Autorizado	Una persona logra acceso físico o lógico sin permiso a una red, sistema, aplicación, datos u otros recursos.
Verificación y Validación	Garantizar mediante firmas electrónicas de 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)	Es un grupo de anfitriones (host) con un conjunto común de requerimientos que se comunican como si estuvieran adjuntas al mismo dominio de difusión independientemente de su locación física. Una VLAN tiene los mismos atributos que una LAN física, pero esta permite que terminales destinatarias se agrupen aunque no estén ubicadas en el mismo conmutador de red.
Red Virtual Privada (VPN)	Una red privada virtual es una red lógica que se establece sobre una red física existente y que normalmente no incluye todos los nodos presente en la red física.
Virus	Es un programa de auto-replicación, generalmente con intención maliciosa que se ejecuta y se propaga modificando otros programas o archivos.
Vulnerabilidad	Es cualquier debilidad dentro de la infraestructura que pueda ser utilizada para proporcionar una “puerta” a la introducción de una amenaza.

1.4. Documentación clave del Concesionario/Agente Operador

1.4.1. Identificación de riesgos.

A través de la presente normativa se especifican las partes/componentes de la red que requieren la mayor cantidad de recursos dirigidos a la seguridad. Cada Concesionario/Agente Operador tendrá alguna porción de su funcionalidad básica dependiente en la información tecnológica y debe ser una parte de su TI. 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 tiene que ser considerado como el primer paso en un análisis de riesgo que debe ser usado como una base de las políticas de seguridad de la información.

NOTA. En base a las políticas de seguridad, LOTBA define lo siguiente como información sensible y no debe interpretarse como si el Concesionario/Agente Operador no pudiese adoptar otros criterios adicionales:

- Contadores electrónicos contables, según estándares técnicos "REQUISITOS Y CARACTERISTICAS DE FUNCIONAMIENTO DE MÁQUINAS ELECTRÓNICAS Y/O ELECTROMECANICAS DE JUEGOS DE AZAR" y "SISTEMA DE MONITOREO Y CONTROL ON LINE ("SMCO") Y SISTEMAS DE VALIDACIÓN DE TICKET/VOUCHER (TITO)"
- Eventos críticos según estándares técnicos "REQUISITOS Y CARACTERISTICAS DE FUNCIONAMIENTO DE MÁQUINAS ELECTRÓNICAS Y/O ELECTROMECANICAS DE JUEGOS DE AZAR" y "SISTEMA DE MONITOREO Y CONTROL ON LINE ("SMCO") Y SISTEMAS DE VALIDACIÓN DE TICKET/VOUCHER (TITO)".
- Los datos personales de jugadores conforme lo definido por la ley 25.326 (habeas data) o la que la reemplace en el futuro.
- Los siguientes datos de tickets: Código de validación, tipo, importe, máquina, locación, fecha de emisión y expiración.
- Las transacciones de los sistemas de gestión de sala asociadas a créditos canjeables o no canjeables y las referentes a valores monetarios.
- Logs de auditorías.

1.4.2. Políticas de Seguridad de la Información (prevención).

El Concesionario/Agente Operador deberá contar con una política de seguridad para identificar, documentar, y dar soporte a la seguridad de la red. El desarrollo de la política debe ser fundamentada sobre un detallado análisis de riesgo y del rendimiento. El documento de la política debe ser desarrollado, implementado y mantenido por el Concesionario/Agente Operador y debe:

a) Estar formalmente documentado y regularmente revisado.

b) Definir las responsabilidades de los usuarios/empleados, y establecer consecuencias por el fallo de no seguir la política, y adicionalmente:

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

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

iii. Definir los requerimientos de protección de acuerdo con la evaluación del riesgo.

iv. Incorporar capacitación para concientizar a los empleados, sobre los pasos a seguir desde su implementación y seguimiento.

1.4.3. Política de Respuesta de Incidentes (PRI).

El Concesionario/Agente Operador deberá contar con una Política de Respuesta de Incidentes, la cual es esencial para asegurar que las amenazas a la seguridad de la red son respondidas a tiempo y de manera efectiva en caso de que las medidas preventivas fallen. El Concesionario/Agente Operador deberá desarrollar, implementar, y mantener un documento PRI y deben:

a) Estar formalmente documentados y renovarse anualmente

b) Definir roles y responsabilidades durante un incidente.

c) Definir un plan de comunicaciones interno y externo.

1.4.4. Plan de Recuperación de Desastres (PRD)

El Concesionario/Agente Operador deberá establecer prácticas y procedimientos de alto nivel, para abordar un evento de falla critica en la infraestructura y mitigar el daño en caso de que las medidas preventivas de seguridad de red fracasen ante la protección de un ataque. Se debe desarrollar, implementar, y mantener por parte del Concesionario/Agente Operador un documento detallando el Plan de Recuperación de Desastres y asegurar que:

a) El personal de Tecnología de la Información (en adelante TI) esté entrenado y familiarizado con los procedimientos.

b) Se realice el correspondiente respaldo de datos (backup) regularmente.

c) Contar con centros de datos múltiples.

d) Se utilicen sistemas de alta disponibilidad que mantengan los datos, el sistema y sus correspondientes réplicas.

CAPITULO 2

2.1. Dispositivos de Red

2.1.1. Tipos y Descripción de los Dispositivos de Red.

a) Hubs: son los dispositivos de red más simples, y simplifican la difusión de la misma información a todos los puertos conectados incluyendo los puertos de origen. 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 a través de un cable de par trenzado. Además de los puertos para conectar las 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): múltiples conmutadores pueden ser utilizados para crear redes más grandes. A pesar de ser similares en apariencia y sus idénticas conexiones físicas a computadoras, los conmutadores ofrecen ventajas operacionales significativas 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 (en adelante MAC) de los dispositivos conectados a éste para determinar el puerto correcto. Una dirección MAC es un número único que está programado dentro de toda placa de red (en adelante NIC). Al reenviar los datos solamente al sistema para el cual los datos están dirigidos, el conmutador disminuye la cantidad de tráfico en cada enlace de red.

c) Puentes (Bridges): 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 de la cual recibió los datos, este puede reenviar los datos a otras redes a las cuales el puente está conectado. Si la dirección no está al otro lado del puente, el paso de los datos es bloqueado. Los puentes reconocen las direcciones MAC de los dispositivos en las redes conectadas analizando el tráfico de la red y registrando la red que origina el tráfico.

d) Routers (Enrutadores): son dispositivos de red que dirigen los datos entre una red de

computadoras más allá de los dispositivos conectados directamente, examinando los datos en cuanto estos arriban. Los routers son capaces de determinar la dirección de destino, usando tablas de ruteo definidas, el router determina la mejor vía para que los datos continúen su viaje. Los enrutadores usan las direcciones de red configuradas en el software para tomar las decisiones.

e) Gateways (Puerta de enlace): es un dispositivo que permite interconectar redes con protocolo y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo utilizado en la red de destino.

f) Punto de Acceso Inalámbrico (en adelante WAP): son dispositivos de red que permiten a las terminales Wi-Fi conectarse a una red cableada, sirviendo como enlace entre los segmentos cableados e inalámbricos de una red.

g) 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.

h) Tarjeta de Interface de Red (en adelante NIC): son los mecanismos por los cuales las computadoras se conectan a una red.

2.2. Controles de Acceso Físico y de Seguridad

Se entiende por seguridad física a la capacidad de permitir o negar el uso de un recurso particular por una entidad individual a través de maneras físicas. La seguridad física es un importante componente de la protección de cualquier red. Controles de acceso físico son características de seguridad que controlan cómo los usuarios y los sistemas se comunican e interactúan con otros sistemas y recursos, y estos sirven para protegerlos de accesos no autorizados. La seguridad física de la red debe prevenir situaciones tales como robo, sabotaje, vandalismo, accidentes y desastres ambientales.

2.2.1. Acceso a los data centers.

Se deberá implementar un mecanismo de acceso al data centers, utilizando puntos de entrada con llave y/o un sistema de tarjetas, biométricos, etc., capaz de registrar y/o controlar todas las entradas a los cuartos en los cuales se alojen los sistemas que contengan información sensible.

Se deberá llevar un control sobre los registros a fin de detectar anomalías en los patrones de acceso.

2.2.2. Seguridad de Racks/Gabinetes de Servidores.

Los gabinetes/racks deben estar asegurados bajo llave para crear una barrera física de acceso a los servidores. El acceso deberá estar restringido solo a personal autorizado.

2.3. Puertos Físicos y Conexiones por Cable Seguridad del puerto Ethernet (Network Jack).

Los puertos Ethernet deben estar deshabilitados cuando no estén en uso, de acuerdo a las siguientes medidas preventivas:

a) Aislamientos de redes.

b) Procedimiento Administrativo, (VLAN "muerta").

c) Estar dentro de una caja con llave.

d) Las peticiones y aprobaciones para la activación de los puertos Ethernet deben ser registradas por el personal de tecnología de la información (IT). El Concesionario/Agente Operador deberá mantener y auditar regularmente un registro de puertos Ethernet habilitados.

2.3.2. Dispositivos de Red externos

Para los dispositivos de red externos al data center tales como enrutadores, firewalls, conmutadores, etc., el acceso a los mismos debe ser restringido al personal autorizados y ser alojados en un ambiente seguro y deberán contar alguna de las siguientes medidas: cerradura, lectura biométrica, lector de tarjetas.

2.3.3. Servicios y Puertos no Necesarios.

a) Los dispositivos de red deben tener apagados los servicios no necesarios, no utilizados y deshabilitados los puertos no esenciales.

b) Debe existir un Diseño de red, el que debe respetarse a fin de garantizar los apropiados controles de seguridad en las nuevas configuraciones de red.

2.4. Recuperación de Desastres y Redundancia (Físico)

2.4.1. Recuperación de Desastres.

Redundancia de red implica tener disponibilidad de recursos en caso de fallas. Recuperación de desastres significa tener un plan en caso de fallos catastróficos para retornar rápidamente acceso a los recursos. La red debe utilizar los siguientes elementos para admitir la recuperación de desastres y la redundancia:

a) Hardware Redundante – La red debe utilizar múltiples partes de hardware que operan paralelamente. En caso que uno falle, el otro continuará la función.

b) Alta-Disponibilidad – La red debe emplear múltiples partes de hardware de manera que si el componente hardware primario falla, el otro secundario se hará cargo.

c) Hardware Intercambiable (en inglés Colds Spares) – Se deben mantener copias exactas del hardware, de manera que en caso de falla, el hardware puede ser intercambiado.

d) Espejado (Mirroring) – La red debe utilizar un espejado de la información crítica. El espejado aplica típicamente 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) Data center de contingencia – La red debe emplear múltiples centros de datos o sitios, es decir un sitio primario y otro secundario. El sitio secundario puede ser utilizado en caso de una emergencia mayor y/o desastre natural u otro desastre en el sitio primario.

Deberá tener una reflexión virtual del sitio actual con los sistemas esenciales listos para ser activado en cualquier momento.

En relación a los centros de respaldo de datos, REFIERASE a “centro de contingencia” requerido en el estándar técnico para los sistemas de monitoreo y de control on line y sistema de validación de tickets voucher (TITO).

2.4.2. Plan de Recuperación de Datos

El Concesionario/Agente Operador deberá contar con un Plan de recuperación de desastres (en

adelante, DRP) el cual documentará cuidadosamente todos los métodos que se utilizan para respaldar la recuperación de desastres de la red. Este plan también debe documentar la información de contacto esencial y debe detallar los pasos necesarios para afectar una recuperación completa de la red. Todos los miembros claves y la alta gerencia deben tener múltiples formas de acceso al documento de DRP, tanto en formato electrónico como impreso, y el plan debe revisarse con frecuencia para abordar los cambios en los sitios, equipos, procedimientos y personal.

2.4.3. Copia de seguridad de la red.

El Concesionario/Agente Operador deberá contar con los siguientes elementos para la copia de seguridad de la información que garantice la seguridad de la red:

a) definir los niveles necesarios de información de respaldo y documentar un plan de recuperación ante desastres;

b) contar con registros precisos y completos de las copias de respaldo y procedimientos de restauración documentados;

c) el grado y la frecuencia de las copias de seguridad deberán reflejar los requisitos de la organización, los requisitos de seguridad de la información involucrada, la importancia de la información para la operación continua de la explotación de las salas, y otros requerimientos que podrá efectuar LOTBA ;

d) las copias de seguridad deben resguardarse a una distancia suficiente para escapar de cualquier daño por desastres en el sitio principal, para permitir su recuperación de manera oportuna;

e) se debe proporcionar a la información de respaldo el mismo nivel de protección física y ambiental aplicados en el sitio principal; los controles aplicados a los medios en el sitio principal se extenderán para cubrir el sitio de respaldo;

f) los medios de respaldo deben ser probados regularmente para asegurar que se pueda confiar en ellos para el uso de emergencia cuando sea necesario; estas pruebas deberán efectuarse como mínimo, una vez por año;

g) los procedimientos de restauración se verificarán y probarán periódicamente para garantizar que sean efectivos y que puedan completarse dentro del tiempo asignado en los procedimientos operativos para la recuperación;

CAPITULO 3

3.1. Protocolos y Comunicaciones de la red

3.1.1. Protocolos de Red.

Los siguientes protocolos de red son los usados comúnmente:

a) UUCP (UNIX-to-UNIX Copy Protocol) – 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 del conjunto de protocolos TCP/IP. TCP asegura que los datos arriben intactos y completos, mientras UDP solamente envía paquetes. TCP es usado para todo lo que tiene que arribar en forma perfecta y UDP es usado para funciones como transmitir media y videoconferencia.

c) SNMP (Protocolo de Administración de Red Simple) – protocolo de monitoreo y control de red que es parte del conjunto de protocolos TCP/IP.

d) RMON (Monitoreo Remoto) – mejora del protocolo SNMP que agrega un conjunto completo de capacidades de monitoreo de red.

e) DHCP (Protocolo de Configuración de Anfitrión (host) Dinámico – es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente.

f) FTP (Protocolo de transferencia de archivos): protocolo utilizado 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.

b) Toda comunicación de datos confidenciales debe incorporar un esquema de detección y corrección de errores para asegurar que los datos son transmitidos y recibidos con exactitud.

c) (SYS LOG) La red debe ser capaz de detectar y mostrar ciertas

condiciones. Estas condiciones serán registradas en un registro de errores que puede ser mostrado o impreso 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 claves.

3.2. Firewalls

3.2.1. Requisitos para la implementación de firewalls.

Los siguientes son los requisitos a aplicar en la implementación de un firewall:

a) Se implementará tecnología Firewall en los bordes de la red para proteger contra el acceso no autorizado a los activos de información internos.

b) Todo tráfico externo y de zona desmilitarizada (DMZ) debe ser dirigido a través de los dispositivos de firewall.

Las siguientes reglas del tráfico de red deben incluir pero no se limitan a las siguientes:

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 pública 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., deberán ser bloqueados.

ix. Cualquier fuente de paquetes ruteados 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.

c) Las tecnologías de administración remota de firewall deben ser mediante comunicaciones cifradas o no permitidas en su totalidad.

d) Las políticas de Firewall deben ser revisadas, ensayadas y auditadas con frecuencia y documentados.

3.2.2. Múltiples Redes.

Cuando un servidor se utilice en conjunto con otras redes, todas las comunicaciones, incluyendo acceso remoto, deben pasar por lo menos un firewall de aplicación y no deberán tener una instalación que permita un camino de red alterno. Solo estará permitido un camino de red alterno para propósitos de redundancia, y este también deberá pasar por lo menos un firewall de aplicación.

NOTA: En casos que por cuestiones de diseño el sistema requiera una solución alternativa, LOTBA lo analizará en cada caso.

3.2.3. Reportes de Auditoria del Firewall. (SYS LOG)

La aplicación firewall debe mantener un reporte de auditoría que incluya la siguiente información:

a) Todos los cambios de configuración del firewall.

b) Todos los intentos de conexión exitosos y sin éxito a través del firewall.

c) Las direcciones IP de origen y destino y los números de puertos para ingresar el tráfico.

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

e) Un parámetro configurable "intentos de conexión fallidos", debe ser utilizado para denegar pedidos de conexión futura en caso de que el parámetro definido se exceda.

Nota: si la capacidad del reporte de auditoría se completa se debe generar un evento de error que lo indique y el Concesionario/Agente Operador deberá tomar una acción correctiva en un plazo de dos (2) horas.

3.3. Protección de Contraseñas e Inicios de Sesión

3.3.1. Contraseñas y configuraciones de los dispositivos.

a) Las contraseñas de los dispositivos deben ser cambiadas inmediatamente antes o luego de la instalación del mismo y debe ajustarse a los requerimientos establecidos por la política de seguridad de la red;

b) Los dispositivos de red deben ser configurados para retener su configuración actual durante un proceso de reinicio o restablecimiento;

c) Las contraseñas administrativas (usuarios con prerrogativas elevadas) deben ser cambiadas regularmente, como mínimo cada 120 días.

d) Sólo se deben utilizar las cuentas individuales que están asignadas únicamente a un individuo – no se deben usar cuentas genéricas o compartidas, excepto para aquellas cuentas usadas para acceso solo de lectura como se describe en otras partes de esta norma;

NOTA: En casos que por cuestiones de diseño el sistema requiera una solución alternativa, LOTBA lo analizará en cada caso.

e) Se debe remover el acceso de los empleados que hayan sido despedidos o suspendidos dentro de 48 horas hábiles de la notificación;

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

g) Los umbrales 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 umbral se excede, la cuenta debe requerir intervención administrativa para desbloquear;

los siguientes criterios:

1) 8 – 14 caracteres de largo;
2) Una combinación de por lo menos tres de los siguientes componentes:
    a) Letras mayúsculas
    b) Letras minúsculas
    c) Números
    d) Caracteres especiales
3) No ser parte del nombre de inicio de sesión;
4) No ser parte de una contraseña previa,
5) Debe evitar información personal del usuario;
6) No ser igual a ninguna de las 8 (ocho) contraseñas utilizadas anteriormente.

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 específico uso y debe existir una técnica de autenticación adecuada para sustanciar la identidad reclamada por el usuario.

a) Los IDs de usuario deben ser capaces de rastrear las actividades del individuo responsable. Las actividades de usuarios comunes no deben ser realizadas desde cuentas con privilegios mayores que los necesarios para la tarea. En circunstancias especiales donde es clara su necesidad, puede utilizarse un ID compartido por un grupo de usuarios o una función específica de trabajo. Sólo se podrá permitir el uso de IDs genéricos en el caso de que las funciones accesibles o acciones llevadas a cabo por el ID no requieran rastreo. (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) Cuando se requiera una autenticación fuerte y verificación de identidad, se recomiendan métodos de autenticación alternativos a las contraseñas, como tarjetas inteligentes, tokens, o medios biométricos.

3.4. Protección de Multi-capa

La protección de capas-múltiples debe ser implementada dondequiera y cuando sea

posible. Las 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.

NOTA: En casos que por cuestiones de diseño el sistema requiera una solución alternativa, LOTBA lo analizará en cada caso.

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 datos/información confidencial o sensible, tal como indica en la sección 1.4.1 de éste estándar técnico

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, contemplando además los futuros desarrollos tecnológicos que sean adoptados por la industria y considerados como mejores prácticas de IT:

a) IPSec – Es 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 dos estaciones-extremas o red sobre un medio de comunicaciones no- confiable.

b) (SSH) (Secure Shell) – Debe ser implementado solamente para la administración remota de datos/información confidencial y 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 implementadas en ambientes donde el cifrado de la capa enlace de datos no es una solución práctica para mantener y operar. Se puede implementar tecnología VPN usando IPSec o cifrado SSL, independiente de una tecnología de comunicaciones capa-enlace particular.

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) Secure /Multipurpose Internet Email Extension (S/MIME) – Es una mejora a la seguridad basado en estándares para asegurar correo electrónico y archivos adjuntos que proporciona una autenticación sólida mediante firmas digitales.

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

La información de la llave pública puede mantenerse en servidores de calve públicas o internas de PGP.

h) Infraestructura de la Llave Publica (PKI) – Funcionalidad técnica basada en PKI está definida por el estándar X.509 y sus extensiones.

3.5.3. Disco (almacenamiento) Encriptación.

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

b) Bases de datos que son utilizadas para almacenar información sensible o protegida debe ser configurada para habilitar encriptación por defecto. La encriptación de campos sensibles de las bases de datos 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 en dispositivos de almacenamiento directamente adjuntos (DAS), y todos dispositivos de almacenamiento portables, 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 – *cifra todos los datos en un disco duro para un dispositivo cliente. Esto incluye todo el sistema operativo, las aplicaciones y los datos / información. El software de cifrado de disco completo contiene componentes que son independientes del sistema operativo y se ejecutan antes de que se cargue el sistema operativo, así como la autenticación. El sistema se vuelve ininteligible e inutilizable en caso de un delito cibernético o terrorismo.*

i. *Encriptación de Disco Completo debe tener las siguientes funciones:* Autenticación de Pre-Arranque laptops / PC's de escritorio; funciones de encriptación basadas en archivos y carpetas integradas dentro del sistema operativo; soporte de inicio de sesión único; 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) – permite cifrado para archivos o carpetas específicos. Las soluciones de cifrado de archivos proporcionan seguridad automática ya que cada nueva capacidad de cifrado de archivos / carpetas se debe activar / desactivar manualmente.

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 adición a 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 pérdidas 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 sino también prescindir de copias de seguridad y medios de archivo.

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

i. *La encriptación de almacenamiento masivo (SAN/NAS) debe 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".

NOTA: En casos que por cuestiones de diseño y performance del sistema se requiera una solución alternativa, LOTBA lo analizará en cada caso.

f) Confidencialidad de la información Sensible – el concesionario/Agente Operador deberán suscribir los correspondientes acuerdos de confidencialidad que garanticen el uso correcto de la información sensible y se asegure su inviolabilidad.

3.5.5. Longitud Mínima de claves de Encriptación

El mínimo ancho (tamaño) de las claves de encriptación debe ser de 128 bits para algoritmos simétricos y 1024 bits para llaves públicas.

3.5.6. Manejo de claves de Encriptación.

Debe haber implementado un método seguro para el cambio del conjunto de claves de encriptación actuales.

3.5.7. Almacenamiento de clave 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

3.6.1. Declaración General.

Las conexiones externas a redes operacionales deben ser dirigidas a través de puertas de enlace (gateways) seguras y protegidas por al menos uno de los siguientes métodos de encriptación, como sea aplicable:

a) Seguridad en la Capa de Transporte (Transport Layer Security - TLS) o Capa de Socket Seguro (Secure Socket Layer - 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 a la autenticación de cliente usando los servicios provistos por las Autoridades Certificadoras. El uso de SSLv3 y TLSv1.1 son considerados obsoletos.

b) La seguridad IP (IPSec) debe ser utilizada para extender el protocolo de comunicaciones IP, proporcionando confidencialidad de extremo a extremo para los paquetes de datos que viajan por 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) Las 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 son IPSec, L2TP, IKEv2, SSTP, etc..

d) Remote Authentication Dial-In User Service (RADIUS) es un protocolo cliente/servidor que habilita la comunicación de los servidores de acceso a la red con el servidor central para autenticar y autorizar accesos remotos a los sistemas o servicios, se debe utilizar una fuerte autenticación para sistemas con módems dial-up.

e) Se deben deshabilitar y retirar los módems Dial-up de las estaciones de trabajo. Se debe implementar hardware o herramientas de escaneo de inventario para verificar la presencia y configuración de utilidades de marcado (dial) y módems. Cualquier uso de sistemas de modem dial-up deben ceñirse a las políticas aceptadas por el Concesionario/Agente Operador que pueden incluir:

   i. Una registro completo y actualizado de todo el personal autorizado con privilegios de acceso a modem.

   ii. Desconexión automática luego de un período especificado de inactividad. Los parámetros de inactividad deben ser determinados por el Concesionario/Agente Operador en línea con las necesidades operacionales.

   iii. Utilización de tokens de seguridad.

   iv. Terminación inmediata de privilegios de acceso modem luego de una transferencia de empleo, re- asignación funciones, o extinción del vínculo laboral.

f) Aquellos con autorización para conectarse de forma externa, una vez que se haya otorgado permiso para conectarse, deberá utilizar una autenticación robusta.

g) Las conexiones externas deben ser removidas cuando ya no sean requeridas. Los componentes claves de la red deben ser deshabilitados

o removidos para prevenir reconexión inadvertida.

3.7. Programas de Protección Antivirus y Malware

3.7.1. Protección de Antivirus y Malware.

Los programas de antivirus y malware utilizados con propósitos de seguridad de la red deben:

a) Ser mandatorios en todos los sistemas.

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

c) Incluir tanto el escaneado del sistema de archivos como el procesamiento en tiempo real.

3.8. Parches y Actualizaciones del Software

3.8.1. Declaración General.

Los Concesionario/Agente Operador deben desarrollar e implementar procedimientos escritos que delineen los roles y responsabilidades para la administración de parches y actualizaciones para el software que cubra las siguientes actividades:

a) Se debe 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) Los parches deben ser instalados y validados en un ambiente de prueba antes de su introducción a un ambiente productivo. 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) 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 sermonitoreados, cuando sea posible.

d) Las configuraciones de sistema deben ser respaldados antes de la

instalación de los parches.

NOTA: Es de aplicación lo prescripto en el artículo 3.10.2. g y para actualizaciones o parches del "SMCO", sistemas de bonificación y sistemas promocionales, el Concesionario/Agente Operador deberá solicitar autorización previa.

3.9. Recuperación de Desastres (Lógico)

3.9.1. Declaración General.

La recuperación de desastres tiene como objetivo garantizar que todos los datos críticos se puedan recuperar a pedido y que se pueda volver a un estado utilizable de la manera más rápida y eficiente posible.

La planificación, la ejecución y las pruebas efectivas de contingencia son esenciales para mitigar el riesgo de falta de disponibilidad del sistema y del servicio.

3.9.2. Planificación de Recuperación de Desastres.

Los componentes del planeamiento de recuperación de desastres y contingencia deben contemplar los siguientes criterios:

a) Se deberá contar con un continuo análisis de impacto del negocio.

b) Se deben implementar controles preventivos y de mantenimiento para reducir los efectos de las interrupciones del sistema y aumentar la disponibilidad del mismo.

c) Se deben implementar estrategias de recuperación exhaustivas para garantizar que los sistemas se puedan recuperar rápida y efectivamente después de una interrupción. Estas estrategias deben incluir una gestión adecuada de la copia de seguridad, las replicaciones y los sistemas de conmutación por error.

d) Se debe desarrollar y cumplir un plan de contingencia que debe contener una guía y procedimientos detallados para restaurar los sistemas y / o datos dañados.

e) Las pruebas planificadas, la capacitación y los ejercicios de planes de contingencia deben realizarse al menos una vez al año.

f) Los planes de contingencia deben ser documentos vivos que se actualicen regularmente para mantenerse actualizados 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 política de seguridad de las computadoras, política de uso aceptable, o prácticas 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. Criterios mínimos

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 Concesionario/Agente Operador 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.

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 políticas 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 concesionario/agente operador, 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.

3.11. Escaneando de Vulnerabilidades

3.11.1. Declaración General.

E l escaneado de red y host, debe ser usado para realizar pruebas de vulnerabilidades en dispositivos de red interna, aplicaciones y defensas del perímetro de red. Deberá dicho escaneado respetar la política de seguridad y estándares vigentes.

3.11.2. Herramientas para el Escaneado de Vulnerabilidades.

Cuando sea técnicamente posible, una herramienta de escaneado de vulnerabilidades automático debe ser usada para escanear la red.

3.11.3. Escáner de Vulnerabilidad.

Los escáneres de vulnerabilidad tendrán 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 políticas de seguridad válidas cuando son usadas durante la instalación de seguridad del dispositivo y certificación.
e) Usar cautela en el escaneo para verificar la operación propia dedispositivos IDS/IPS.
f) Idealmente el escaneado de vulnerabilidad debe incluir ambos escaneados la red y nivel de aplicación.

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 (Log)

3.12.1. Registro de Seguridad.

a) Las capacidades de registro se habilitarán en los dispositivos que sean compatibles.
b) Los registros deben revisarse, en una frecuencia determinada y documentada por el Concesionario/Agente Operador. Esto incluye la verificación manual de las herramientas de análisis de registro automático.
c) Los registros se realizarán localmente y se reflejarán periódicamente en un servidor centralizado para evitar la manipulación de los datos a nivel del sistema.
d) Todos los dispositivos de red aprovecharán los servidores de protocolo de tiempo de red (NTP) para estandarizar las marcas de tiempo para los datos de registro a fin de garantizar que se pueda recrear una línea de tiempo adecuada en caso de un incidente.

3.12.2. Sincronización de Reloj (NTP)

Para facilitar el registro, los relojes de todos los sistemas de procesamiento de información relevantes dentro de una organización o dominio de seguridad se sincronizarán con una fuente de tiempo acordada y precisa.

3.13. Acceso Remoto

3.13.1. Declaración General.

El acceso remoto se define como cualquier acceso al sistema fuera de la red segura o de confianza. La seguridad del acceso remoto será responsabilidad del Concesionario/Agente Operador.

3.13.2. Requerimientos de Acceso Remoto.

Una red puede utilizar acceso remoto controlado por contraseña siempre y cuando se cumplan los siguientes requisitos:

a) Se mantendrá un registro de actividad del usuario de acceso remoto como se describe a continuación;
b) No se permitirá ninguna funcionalidad no autorizada de administración remota de usuarios (agregar usuarios, cambiar permisos, etc.);
c) No se permitirá el acceso no autorizado a una base de datos que no sea la recuperación de información utilizando las funciones existentes;
d) Se debe instalar un filtro de red (firewall) para proteger el acceso.

NOTA: Se reconoce que el fabricante del sistema puede, según sea necesario, acceder de forma remota a la red y sus componentes asociados para fines de soporte de producto y usuario, siempre y cuando esté permitido por el Concesionario/Agente Operador y debidamente informado a LOTBA. Asimismo en caso de utilizar una herramienta propia o de tercero, deberá requerírsele al proveedor del sistema un reporte de auditoria.

3.13.3. Reportes de Auditoria de Acceso Remoto.

El servidor de red debe mantener un registro de actividad automáticamente o tener la capacidad de ingresar manualmente los registros que representan toda la información de acceso remoto. Los registros de acceso remoto incluirán mínimamente lo siguiente:

a) Nombre de inicio de sesión del usuario.

b) Fecha y hora en que la conexión fue hecha.

c) Duración de la conexión.

d) Actividad mientras está conectado, incluidas las áreas específicas a las que se accedió y los cambios que se realizaron.

CAPITULO 4

4. *REDES INALÁMBRICAS*

4.1. Consideraciones Únicas

4.1.1. Declaración General.

La interfaz inalámbrica define el límite de comunicación entre dos entidades, como una pieza de software, un dispositivo de hardware o el usuario final. También puede proporcionar un medio de traducción entre entidades que no hablan el mismo idioma. Esta sección trata sobre las interfaces de software que existen entre componentes de hardware y software separados que componen el sistema inalámbrico, y que proporcionan un mecanismo programático de forma tal que estos componentes pueden comunicarse.

4.1.2. Protocolo de Comunicación

Cada componente de una red inalámbrica funcionará según lo indicado por el protocolo de comunicación implementado. Toda comunicación entre el servidor y el cliente móvil utilizará una autenticación apropiada y protocolos criptográficos para proporcionar autenticación mutua del dispositivo móvil y el servidor.

4.1.3. Servidor Inalámbrico Usado con Otros Sistemas.

En caso de que el servidor inalámbrico se utilice junto con otros sistemas; (es decir, sistemas de monitoreo y control en línea, sistemas de validación de boletos, sistemas progresivos, etc.) incluido el acceso remoto, todas las comunicaciones pasarán por al menos un firewall de aplicación suficientemente robusto y no deberán tener una instalación que permita una ruta de red alternativa a menos que la ruta alternativa cumpla con los requisitos de este documento y tenga seguridad independiente (es decir, las claves no son las mismas que otras redes).

4.1.4. Seguridad Física de Red Inalámbrica.

Una red inalámbrica debe cumplir con los siguientes requisitos mínimos:

a) Los Puntos de Acceso Inalámbricos (WAP) se ubicarán físicamente de forma que no estén al alcance del público en general;

b) Si lo anterior no es factible, todas las salidas Ethernet expuestas serán desactivadas;

c) La red inalámbrica deberá diseñarse para ser una red independiente (aislada) de acuerdo con técnicas de estratificación múltiple mencionadas anteriormente;

d) La red debe soportar el monitoreo en busca de evidencia de acceso no autorizado. Si se ha detectado el acceso, la red debe afirmar los controles apropiados para bloquear o deshabilitar el punto de entrada sospechoso, si es posible, ynotificar al Concesionario/Agente Operador; y

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

4.1.5. Software de Seguridad de Redes Inalámbricas.

Una red inalámbrica debe:

a) Ser diseñada o programada de tal manera que solo se comunique con clientes / dispositivos inalámbricos autorizados. El software transferido entre el servidor y el cliente / dispositivo debe implementarse utilizando un método que enlace de forma segura el cliente / dispositivo al servidor, de forma que el software solo pueda ser utilizado por clientes/ dispositivos autorizados. Si se usan certificados, claves o semillas, no deben estar codificados y deben cambiarse automáticamente a lo largo del tiempo como una función del enlace de comunicación;

b) Emplear cifrado y fuerte autenticación de usuario, con algún método tal como: 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 válida.

d) Validar los clientes/dispositivos en intervalos de tiempo predefinidos con por lo menos un método de autenticación como se describió anteriormente;

e) Mantener un registro (base de datos) de clientes / dispositivos autorizados con los que se pueda comunicar. Este registro incluirá el nombre del cliente / dispositivo, una identificación única del cliente / dispositivo y el correspondiente identificador de hardware (MAC);

f) Instalar y mantener un firewall de inspección de paquetes con estado independiente, que aislará los puntos de acceso de otros componentes de red que el Concesionario/Agente Operador haya desplegado;

g) Ocultar el identificador de conjunto de servicios (SSID) para que las redes a las que está conectado no sean visibles;

h) Cerrar las sesiones activas si la autenticación del usuario ha superado la cantidad de intentos fallidos;

i) Tendrá la capacidad de generar un informe imprimible de los intentos fallidos de acceso a la red, incluyendo la fecha y hora (timestamp), el nombre del dispositivo, y el identificador del hardware de todos los dispositivos que solicitan el accesos a la red;

j) Deberá implementarse una sólida autenticación de usuario, autorización y cifrado, que validará al usuario contra una base de datos segura. Las comunicaciones entre la red y el dispositivo cliente deben usar protocolos diseñados para asegurar, autenticar y encriptar redes inalámbricas.

802.1x MÉTODOS DE AUTENTICACIÓN RECOMENDADOS		
METODO DE AUTENTICACION	ACRONIMO	AUTENTICADO CONTRA
Protected Extensible Authentication Protocol	PEAP	LDAP, RADIUS, Kerberos o Servidores Microsoft Active Directory, como también bases de datos locales alojadas en un controlador Gateway seguro.
Extensible Authentication Protocol Transport Layer Security	EAP-TLS	
Extensible Authentication Protocol-Tunneled Transport Layer Security	EAP-TTLS	
Virtual Private Network with L2TP/IPsec	VPN	
Point to Point Tunneling Protocol	PPTP	

Secure Sockets Layer	SSL

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

k) Aunque un intruso puede monitorear el enlace de comunicación por aire, se evita que los datos dentro del túnel encriptado sean interceptados mediante la implementación de uno o más de los métodos enumerados en la tabla anterior.

l) No se recomienda el uso de los métodos de protocolo de autenticación extensible (EAP) no tunelizados enumerados a continuación, porque los enlaces de datos inalámbricos podrían verse comprometidos.

802.1X MÉTODOS DE AUTENTICACIÓN NO-RECOMENDADOS	
METODO DE AUTENTICACIÓN	ACRONIMO
Extensible Authentication Protocol	EAP
Extensible Authentication Protocol Message	EAP-MD5
Digest 5	
Lightweight Extensible Authentication Protocol	LEAP

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

4.1.6. Fallas de Componente.

La red inalámbrica tendrá suficiente redundancia y modularidad para solventar una falla de componentes y así evitar la interrupción de las operaciones inalámbricas. Además, habrá copias redundantes de cada registro de auditoría y base de datos del sistema, cuando corresponda, en el servidor inalámbrico con soporte abierto para copias de seguridad y restauración. Esto incluye una red inalámbrica que tiene soporte para la redundancia de failover. Debe realizarse una implementación de esquema de respaldo de acuerdo con la Política de recuperación de desastres.

4.1.7. Requerimientos de Recuperación.

En el caso de una falla catastrófica cuando la red inalámbrica no se puede reiniciar de otra manera, será posible volver a cargar el sistema desde el último punto de respaldo viable y recuperar completamente el contenido de esa copia de seguridad, que debe constar como mínimo de la siguiente información, según corresponda:

a) Eventos Significantes;

b) Información de Auditoria; e

c) Información específica del sitio como los valores únicos de configuración, cuentas de seguridad, etc.

4.1.8. Comunicaciones y Protocolos Inalámbricos.

Cuando corresponda, el estándar IEEE 802.11x se utilizará con redes inalámbricas estándar: IEEE 802.11x (red de área local inalámbrica (WLAN)), IEEE 802.15 (red de área personal inalámbrica (WPAN)) e IEEE 802.16 (red de área metropolitana inalámbrica (WMAN)).

a) La seguridad WLAN se incluye en la capa de transmisión con el borrador del estándar IEEE 802.11i y en la capa de aplicaciones IP con estándares y autenticación basada en políticas y control de acceso.

i. El algoritmo Wired Equivalent Privacy (WEP), que es parte del estándar 802.11, nos era aceptado por considerarse comprometido y no confiable;

ii. El algoritmo Wifi Protected Access (WPA2) y Protected Extensible Authentication Protocol (PEAP) con el estándar de Autenticación de Puerto de Red IEEE 802.1x será aceptado.

iii. WPA2 permite la generación automática de claves por usuario y por sesión a través de 802.1x.

iv. La Pre-Shared Key (WPA-PSK) es susceptible a “ataques de fuerza bruta” (ataques afirmados sobre la repetición). En caso que se utilice, se requerirá también en uso de contraseña fuerte generada aleatoriamente de más de 16 caracteres que contenga todo lo siguiente:

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

b) WLAN Seguridad del Dispositivo de Punto de Acceso Inalámbrico

i. Se deberá cambiar la configuración predeterminada del identificador del conjunto de servicios (SSID)

ii. En caso de deshabilitar la función de difundir el SSID se que requiere que los clientes/dispositivos inalámbricos sean pre-configurados para un punto de acceso específico.

iii. Las contraseñas de acceso a la administración deben cambiarse de su

configuración predeterminada y las claves criptográficas deben cambiarse de la configuración predeterminada de fábrica.

iv. Los dispositivos de punto de acceso se gestionarán a través de herramientas de gestión de red utilizando SNMPv3 o superior. Si la gestión de la red no es realizada por los Concesionarios/Agentes Operadores, se debe deshabilitar SNMP.

v. Los dispositivos de Punto de Acceso deberán operar con un controlador central y deben ser deshabilitados fuera de horario, o cuando no están en uso.

vi. Los puntos de acceso que están conectados a Internet por cualquier medio deben hacer que su tráfico use una LAN virtual (VLAN) y / o una Traducción de direcciones de red (NAT). Las VLAN están cubiertas por IEEE 802.1Q. Se deberá utilizar una VPN para acceder a los recursos internos.

vii. La intensidad de la señal (relación señal-ruido) de los Puntos de Acceso Inalámbricos será auditada y reducida para abarcar solo las áreas deseadas.

viii. El Concesionario/Agente Operador deberá mantener un registro de puntos de acceso inalámbricos autorizados y realizar búsquedas periódicas por puntos de acceso no autorizados que se transmitan dentro de su perímetro de red definido.

c) Los dispositivos inalámbricos de red de área personal (WPAN) utilizados para el acceso a la red, el acceso a Internet basado en la red interna y el software de aplicación deberán:

i. Acogerse al mismo rango de requerimientos de seguridad como los dispositivos cliente WLAN.

ii. Requerir ingreso de PIN u otra autenticación.

iii. Invocar encriptación de enlace en todas las conexiones y transmisiones de difusión.

iv. Utilizar un nivel de potencia necesario para mantener la transmisión localizada en el área inmediata.

v. Requerir contraseñas fuertes para los dispositivos para prevenir el uso no autorizado de dichos dispositivos.

vi. Utilizar encriptación de nivel de aplicación, tecnologías VPN y autenticación.

vii. Desconectarse cuando no estén en uso.

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

e) La tecnología de firewall se implementará en todas las pasarelas (Gateway) de aplicaciones inalámbricas.

CAPITULO 5

5. *RECURSOS DE CÓMPUTO EN LA NUBE*

5.1. Declaración General

La computación en la nube es un modelo que permite acceso de red extendido, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que se pueden aprovisionar y liberar rápidamente con un mínimo esfuerzo administrativo o interacción del proveedor de servicios. Este modelo de nube está compuesto por cinco características esenciales, tres modelos de servicio y cuatro modelos de implementación."

5.2. Consideraciones Generales

5.2.1. Verificación de autenticidad.

Se deberá emplear un mecanismo de verificación de identidad.

5.2.2. Acuerdos de servicio

En caso de que la infraestructura local sea administrada por un tercero se deberá detallar el acuerdo de nivel de servicio y el mismo deberá ajustarse a la política de seguridad establecida por el Concesionario/Agente Operador.

5.2.3. 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, ISO27OO1).

5.2.4. Nubes Privadas on-site.

Nubes privadas on-site son entornos de nube que están totalmente localizados en las instalaciones del Concesionario/Agente Operador.

5.2.5. Seguridad de Nubes Privadas on-Site.

La seguridad de las nubes privadas on-site deberán cumplir con todos lo requisitos establecidos en la presente norma.

5.2.6. Nube Privada Fuera-de sitio.

Una nube privada externa se puede proteger de la misma manera que una nube privada en el sitio. No se pueden hacer suposiciones sobre el nivel de protección otorgado por el proveedor.

5.2.7. Nube Pública.

Ya que la capacidad de construir un túnel puede no existir, en una nube pública todo el tráfico hacia y desde su aplicación podría considerarse información no confiable y sensible y la aplicación debe ser cifrada.

CAPITULO 6

6. INGENIERÍA SOCIAL Y EDUCACIÓN

6.1. Declaración General

6.1.1. Nube Privada Fuera-de sitio.

Ataques de Ingeniería Social incluyen, intrusiones no-técnicas usando información obtenida a través de la interacción humana y basada en trucos para victimizar a un individuo que no familiarizado con las tecnologías y protocolos emergentes. Los operadores de la red deben establecer políticas e implementar los programas de entrenamiento necesarios para atender este tipo de ataques.

6.2. 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 sensible y a quien deben dirigir este tipo de consultas dentro de los Concesionario/Agente Operador.

6.3. Información operacional Disponible

La información operacional disponible debe ser protegida.

Dicha información incluye, 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.

6.4. Seguridad de los Mensajes de Voz

a) Con solo un número de teléfono, un hacker puede acceder a información operacional sensible que ha sido grabada en mensajes de voz, en cuentas de mensaje de voz con contraseñas débiles.

b) El operador de la red debe adoptar y aplicar una política para contraseñas de correo de voz relacionado con el largo y complejidad.

6.5. Correo Electrónico o comunicaciones Dirigidas “Phishing”

Son Correo electrónicos enviados a individuos y grupos dentro de la red de operadores en un esfuerzo de tentar al usuario a revelar información sensible.

Spear Phishing: es una Combinación de intentos estándar de phishing con técnicas de ingeniería social ("Spear Phishing")

a) Se deben integrar dentro de la red dispositivos Firewall para correo no deseado para mitigar las ocurrencias de correos no deseados “phishing” siendo entregados a usuarios internos y externos.

b) El personal debe ser instruido sobre como reconocer posibles correos electrónicos peligrosos.

6.6. Eliminación de Documentos Sensibles

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

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

c) Discos duros y dispositivos de almacenamiento en disco en computadoras y otros equipos electrónicos como fotocopiadoras deben eliminarse 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: La eliminación y/o destrucción de la documentación e información y cualquier manipulación de la documentación sensible debe cumplir por completo con las normas regulatorias vigentes. Estas prácticas deben estar documentadas en la política de seguridad del Concesionario/Agente Operador.

CAPITULO 7

7. AUDITORIAS EXTERNAS SOBRE PRACTICAS DE SEGURIDAD INFORMATICA

LOTBA, tendrá la potestad de realizar las auditorias que considere necesarias tanto sobre el las políticas y prácticas de seguridad informática del Concesionario/Agente Operador, pudiendo contratar un tercero para la realización de estas tareas.

Asimismo, a requerimiento de LOTBA, y cuando Esta lo considere oportuno y necesario, el Concesionario/ Agente Operador deberá realizar auditorías externas sobre sus sistemas, y/o temas asociados a los mismos, comprometiéndose a la comunicación de los resultados o hallazgos que resultasen de las mismas y su posterior subsanación.

SISTEMA DE MONITOREO Y VIDEO VIGILANCIA

Capitulo Único

1. DEFINICIONES Y EQUIPOS DE VIGILANCIA

Los siguientes términos tendrán los significados especificados a continuación:

“Cajas” Es un espacio debidamente asegurado ubicada en una Sala de Juego en la cual debe contar con los medios necesarios para brindar los servicios de cobro y pago. Esta definición no incluye a los KIOSKOS.

“Cámara Dedicada” Es una cámara de video requerida por estos estándares para registrar en forma continua una actividad específica.

“Cámara Dedicada Activada por Movimiento” Es una cámara de video que, cuando detecta actividad o movimiento en un área específica comienza a registrar la actividad en dicha área.

“Cámara PTZ/Domo” Es una cámara de video que posee, como mínimo, capacidades de moverse de un lado a otro, inclinación y acercamiento o características comparables a la mismas.

“Sala de Vigilancia” Es un lugar seguro en una Sala de Juego equipado con monitores de vigilancia grabadoras, selectores de control remoto y demás equipos accesorios utilizados primordialmente para la vigilancia de las Salas de Juegos.

“LOTBA” Lotería de la Ciudad es el Ente regulador en materia de Juegos de Azar en la jurisdicción de la Ciudad Autónoma de Buenos.

“Sistema de Monitoreo y Video Vigilancia” Es uno o varios sistemas de cámaras de video, monitores, grabadoras, servidores de almacenamiento de imágenes, impresoras de video, interruptores, selectores y cualquier otro equipo accesorio usado para la vigilancia en las Salas de Juegos, que permita la visualización y administración de las imágenes, habilitando su captura y/o procesamiento y al cual LOTBA deberá tener acceso.

“Vigilancia de las Salas de Juegos” Es la acción de observar y registrar las actividades que se lleven a cabo en una Salas de Juegos.

“Grabación de video digital" (DVR/NVR/NDVR): "imágenes visuales convertidos en una serie de valores números y almacenados en cinta, disco de video digital u otro medio de almacenamiento, para reproducción posterior.

Nota: La utilización del sistema integral de video vigilancia está regida por el principio de proporcionalidad y razonabilidad, en su doble versión de procedencia y de intervención mínima. La procedencia determina que sólo podrá emplearse cuando resulte adecuado, en una situación concreta, para asegurar la convivencia ciudadana, la utilización pacífica de las vías y espacios públicos, la elaboración de políticas públicas de planificación urbana, así como para la prevención de faltas, contravenciones y delitos y otras infracciones relacionadas con la seguridad pública.

La intervención mínima exige la ponderación en cada caso de la finalidad pretendida y la posible afectación al derecho a la propia imagen, a la intimidad y a la privacidad de las personas, de conformidad con los principios consagrados en la Constitución Nacional y la

2. SALA DE VIGILANCIA

Todo Concesionario / Agente Operador deberá operar su Sistema de Monitoreo y Video Vigilancia desde una Sala de Vigilancia.

3. ACCESOS

El ingreso a la Sala de Vigilancia no deberá ser accesible a empleados no autorizados de las Salas de Juego ni al público en general, el acceso a la Sala de Vigilancia debe estar limitado al personal de vigilancia a los empleados de confianza y demás personal autorizado de conformidad con la política del Concesionario/Agente Operador establecida en su manual de Sistema de Monitoreo y Video Vigilancia. Cualquier representante de la Gerencia de Control de Juegos y Apuestas en el ejercicio de sus funciones podrá tener acceso a la Sala de Vigilancia, siempre que presente la identificación que lo acredita como tal.

4. CONTROL

El equipo de la Sala de Vigilancia debe tener capacidad de controlar los equipos de vigilancia ubicados fuera de la misma.

5. ENERGÍA ININTERRUMPIDA

Todo Concesionario/Agente Operador deberá contar con un sistema de energía ininterrumpida el que debe estar disponible y ser capaz de suministrar inmediata restauración de la energía eléctrica a todos los elementos del Sistema de Monitoreo y Video Vigilancia.

6. MARCAS DE AGUA

El Sistema de Monitoreo y Video Vigilancia debe incluir generadores de fecha y de hora (marca de agua) que posean la capacidad de mostrar la fecha y hora, sala y cámara de los eventos registrados en las grabaciones de video. La fecha y la hora mostradas no deberán obstruir de manera significativa la visión grabada.

7. PERSONAL

Las Salas de Vigilancia deben ser atendidas en todo momento por personal entrenado en el uso del equipo, con conocimiento de los juegos, de las reglas de la casa y de la normativa vigente.

8. OBSTRUCCIÓN DE CAMARAS

Toda cámara de video requerida por estos estándares debe ser instalada de manera que no pueda ser obstruida, alterada o inhabilitada por los clientes o los empleados de las Salas de Juego, excepto que por cuestiones de mantenimiento deban ser atendidas.

9. PROHIBICIÓN

Queda prohibido al personal obstruir intencionalmente el equipo del Sistema de Vigilancia.

10. CÁMARA PTZ O DOMO

En el caso que se utilice una cámara PTZ/Domo para observar las actividades relacionadas con el juego, la cámara debe ser colocada detrás de una cúpula ahumada o con un espejo

que tenga visibilidad de un solo lado o de materiales similares que oculten la cámara de la vista.

11. GRABACIÓN

Toda cámara de video requerida por estos estándares debe tener la capacidad de hacer que su imagen sea mostrada en un monitor de video y sea grabada. El Sistema de Vigilancia debe incluir un número suficiente de monitores, servidores y de grabadoras para mostrar y grabar simultáneamente múltiples actividades de juego, accesos de las salas, sala de conteo y para almacenar las vistas de todas las cámaras.

12. DESPERFECTO Y FALLAS

Se debe reparar cada desperfecto del equipo del Sistema de Monitoreo y Video Vigilancia requerido por estos estándares, dentro de las veinticuatro (24) horas posteriores al descubrimiento del mal funcionamiento. Si el desperfecto no es reparado dentro de este período el Concesionario/Agente Operador debe notificar por escrito al Laboratorio Técnico y Centro de Monitoreo y Control de LOTBA.

13. CÁMARA ALTERNATIVA

En el caso que una Cámara tenga desperfectos, el Concesionario/Agente Operador debe inmediatamente suministrar cobertura con una cámara alternativa o tomar otras medidas de seguridad tales como personal adicional de supervisión de seguridad para proteger la actividad en cuestión, hasta tanto se solucione el desperfecto.

14. PLANOS Y LAYOUT

El Concesionario/Agente Operador deberá presentar los planos con el lay out de la sala en formato digital, utilizando cualquier software de diseño asistido (CAD) con gráficos vectoriales 2D como mínimo, los planos podrán contener varias capas de información y deberán representar las islas de máquinas y demás elementos asociados de forma tal que permita inferirse fácilmente qué número de cámara las registra, deberá indicarse como mínimo los números de los dispositivos de juego o su locación, y las islas en las que se agrupan, como así también nombre, tipo y posicionamiento (área de cobertura) de cada cámara y el sistema plataforma o interfaz que se encuentra alojada la misma. En forma separada se deberá remitir un listado que contenga las distintas cámaras individualizando las MEEJAs que visualiza cada una de ellas.

15. MODIFICACIONES Y CAMBIOS

Todo cambio respecto a los ángulos de enfoque de las cámaras, planos y listados que se produjere debe ser comunicado previo a su ejecución.

16. COBERTURA REQUERIDA. MÁQUINAS TRAGAMONEDAS Y OTRAS ACTIVIDADES LÚDICAS:

16.1 Toda Máquina Tragamonedas deben ser monitoreada por una o más cámaras para suministrar cobertura de todos los clientes y empleados en la MEEJA.

16.2 El área de cajas de la Sala de Juego en la cual se llevan a cabo transacciones de pago y

cobro, debe ser monitoreada por una Cámara Dedicada o por una Cámara Dedicada Activada por Movimiento que provea cobertura con suficiente claridad como para identificar los valores, billetes, fichas y las sumas de los comprobantes (tickets o cualquier otro método alternativo aprobado).

16.3 LOTBA podrá requerir cobertura del sistema de monitoreo y vigilancia en otras áreas o para otras actividades lúdicas, o de otra índole, no incluidas en la presente norma.

16.4 COBERTURA REQUERIDA - CAMARAS DE LA ACTIVIDAD HIPICA

Los Sistemas de Monitoreo y Video Vigilancia de los Concesionarios deben poseer la capacidad para monitorear y grabar todas las áreas en las que se desarrollen actividades hípicas de carreras de caballos SPC en el hipódromo Argentino de Palermo, siendo requeridas, como mínimo los siguientes sectores:

- IDENTIFICACION DE LOS SPC
- CONTROL DOPING
- PISTAS
- DISCO DE LLEGADA

17. - COBERTURA REQUERIDA - CUARTO DE CONTEO

17.1 - Los Sistemas de Monitoreo y Video Vigilancia de los Concesionarios/ Agentes Operadores deben poseer la capacidad para monitorear y grabar todas las áreas en las que se puedan almacenar valores, incluyendo la sala de conteo y todas las áreas en las cuales se puedan almacenar los que no hayan sido contados durante el proceso de drop y de conteo.

17.2 -En caso de poseer balanzas, la cobertura debe ser lo suficientemente clara como para ver cualquier intento de manipulación de los datos registrados.

17.3 – El área de almacenamiento de las cajas metálicas de las mesas de juego debe ser monitoreada ya sea por una Cámara Dedicada o una Cámara Dedicada Activada por Movimientos.

17.4 - Los Sistemas de monitoreo y Video Vigilancia de los Concesionarios/Agentes Operadores deben poseer la capacidad de monitorear y de registrar el cuarto de conteo general, incluyendo todas las puertas que dan al mismo, todas las cajas del drop, las cajas de seguridad y las superficies de conteo y todo el personal del equipo de conteo. El área de la superficie de conteo debe ser continuamente monitoreada por una o más Cámaras Dedicadas durante este proceso.

17.5 - Para las Salas de conteo que utilizan contadores y clasificadores de moneda circulante, como así también fichas, y tokens, el Sistema de Monitoreo y Video Vigilancia deberá poseer la capacidad de monitorear y de grabar todas las áreas en las cuales la moneda circulante, fichas o tokens es recogida, apilada, contada, verificada o almacenada durante el proceso de control. La cobertura de la visión de las máquinas de conteo de moneda circulante, fichas y tokens y de la máquinas de clasificación de moneda circulante, fichas y tokens debe ser lo suficientemente clara de manera que se pueda observar la introducción, extracción y rechazo de las mismas.

18. - COBERTURA REQUERIDA: EXCLUIDOS, AUTOEXCLUIDOS, MENORES y EMERGENCIAS MÉDICAS.

18.1 - Los Sistemas de Monitoreo y Video Vigilancia de los Concesionarios/Agentes Operadores deben poseer la capacidad de monitorear y de grabar, toda situación asociada a la exclusión, autoexclusión y emergencias médicas de personas que se encuentren tanto en los ingresos como dentro de las Salas de Juego.

18.2 - Asimismo el personal de vigilancia deberá tomar todas las medidas necesarias que permitan prevenir el ingreso de aquellas personas que se encuentren excluidos o autoexcluidos, menores de edad y cualquier otra persona que tenga restringido el acceso a las salas de juego por cualquier motivo que fuese.

19. - COBERTURA REQUERIDA: AVERÍAS

Los Sistemas de Monitoreo y Video Vigilancia de los Concesionarios/Agentes Operadores deben poseer la capacidad de monitorear y de grabar, todo aquello asociado con averías/fallas técnicas de las MEEJAs que pudieran afectar sus contadores electrónicos y/o el cálculo del beneficio de las mismas, o cuando la falla/avería tenga como desenlace una incongruencia asociada a los premios o montos establecidos en la tablas de premios de cada MEEJA y que puedan afectar derechos de los ciudadanos.

20. COBERTURA REQUERIDA: PREMIOS

20.1 - Los Sistemas de Monitoreo y Video Vigilancia de los Concesionarios/Agentes Operadores deben poseer la capacidad de monitorear y de grabar, todo aquello asociado con pago de Premios Jackpots o Progresivos y/o todo los incidentes referidos a dichos premios, y que puedan afectar derechos de los ciudadanos.

20.2 - Asimismo deberán resguardar las imágenes que involucren una suma equivalente o superior a Dólares estadounidenses Diez Mil (U$S 10.000)

21. – COBERTURA REQUERIDA: CENTRO DE PROCESAMIENTO DE DATOS

Los Sistemas de Monitoreo y Video Vigilancia de los Concesionarios/Agentes Operadores deben poseer la capacidad de monitorear y de grabar, tanto los accesos, como así también el interior de los centros de Procesamiento de datos, ya sean principales o de contingencia a fin de registrar la actividad acontecida en los mismos.

NOTA: El concesionario/agente operador deberá establecer políticas y/o protocolos para la actuación del personal involucrado en el manejo y accionar del sistema de monitoreo y video vigilancia y de sus componentes que aseguren las coberturas citadas anteriormente.

22. REGISTRO

22.1 - El almacenamiento de las imágenes producidas por la totalidad de las cámaras deben ser resguardadas ininterrumpidamente por un mínimo de quince (15) días, con excepción de las grabaciones previstas en los artículos 18, 19 y 20 de la presente, las que lo serán por un periodo de, al menos, veintiún (21) días.

22.2 - los eventos que por su magnitud resulten ajenos al normal funcionamiento de la sala,

que no se limitan pero incluyen a los anteriormente detallados, deberán ser almacenados en medios ópticos, magnéticos y/o cualquier otro medio de almacenamiento que en el futuro pueda implementarse, pudiendo utilizarse una secuencia de imágenes o un segmento de video a tal fin

22.3 - Todo Concesionario/Agente Operador debe incluir en su manual de Sistema de Monitoreo y Video Vigilancia un procedimiento para el almacenamiento y la identificación de todas las grabaciones de video que se requiere que sean retenidas.

22.4 - El video de un evento grabado, deberá estar disponible para su inmediata visualización por parte de LOTBA.

22.5 - Los Sistemas de monitoreo y Video Vigilancia de Concesionarios/Agentes Operadores deben mantener la capacidad para producir una copia inmóvil o una fotografía de las imágenes contenidas en una grabación de video.

22.6 - El Concesionario/Agente Operador debe mantener un registro que documente los desperfectos que por su naturaleza o magnitud, pudieran afectar el normal control y vigilancia del Sistema de monitoreo y video Vigilancia (como se define en estos estándares). El registro debe especificar la hora, la fecha y la naturaleza de cada desperfecto, las razones de cualquier demora para reparar el desperfecto, la fecha en el que el desperfecto es reparado y donde sea aplicable, cualquier medida alternativa de seguridad que haya sido tomada.

23 COMUNICACIÓN SALAS DE JUEGO - LOTBA

La transmisión de datos se realizará mediante un enlace de comunicaciónCaracterísticas Técnicas de los Sistemas de Monitoreo y Video Vigilancia. El software a instalar en la Sala, deberá permitir:- La visualización en pantalla de hasta dieciséis (16) cámaras en forma simultánea, y la automática ampliación de cada una de ellas según la necesidad.

24.2 - La cantidad de cámaras a instalar dependerá de las características propias de cada sala, debiéndose garantizar la cobertura de la totalidad de las MEEJA autorizadas.

24.3 - Cada Agente operador podrá elegir el tipo de cámaras a utilizar pero deberá garantizar a partir del dictado de la presente que las imágenes obtenidas serán automáticamente digitalizadas en alta resolución (High Definition) o superior, permitiendo su transmisión.

24.4 - Ser capaz de grabar y, posteriormente, ser visto, con un mínimo de 15 (quince) imágenes por segundo, pantalla completa, en tiempo real.

24.5 - Tener un sistema de notificación de fallas que proporcione una notificación audible, así como una notificación visual de cualquier falla en el sistema de vigilancia o en el sistema de almacenamiento de medios de DVR/NVR/NDVR.

24.6 - Tener un sistema de almacenamiento de medios configurado de tal manera que la falla de un solo componente no implique la pérdida de datos del sistema de almacenamiento de medios.

24.7 - Para los sectores, donde no se desarrolle actividad de MEEJAs, las cámaras deberán proporcionar un mínimo de diez (10) cuadros por segundo.

24.8 - Las cámaras deberán contar con nombres normalizados para su mejor identificación.

25 AUDITORIA EXTERNA DEL SISTEMA DE MONITOREO Y VIDEOVIGILANCIA

LOTBA, tendrá la potestad de realizar las auditorias que considere necesarias tanto sobre el Sistema de Monitoreo y Video vigilancia, como así también sobre cualquiera de sus componentes, pudiendo contratar a un tercero para la realización de estas tareas.

Asimismo, a requerimiento de LOTBA, el Concesionario/ Agente Operador deberá realizar auditorías externas sobre sus sistemas, y/o temas asociados a los mismos, comprometiéndose a la comunicación de los resultados o hallazgos que resultasen de las mismas y su posterior subsanación.

APÉNDICE 1 - FIGURAS

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

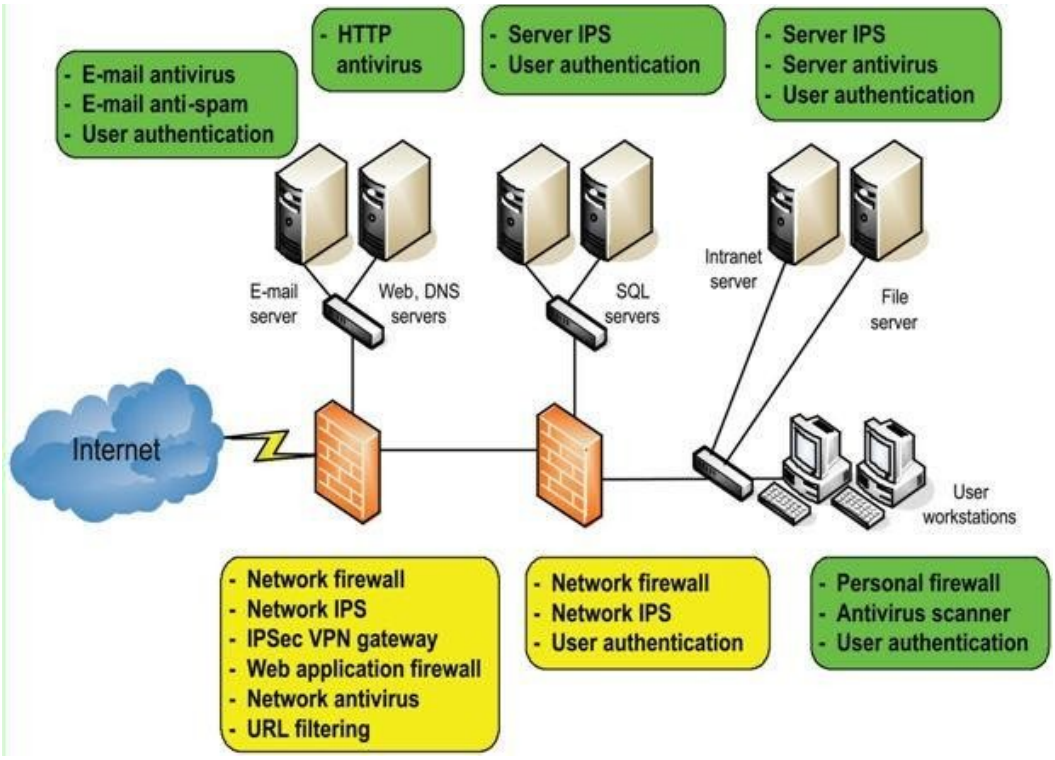
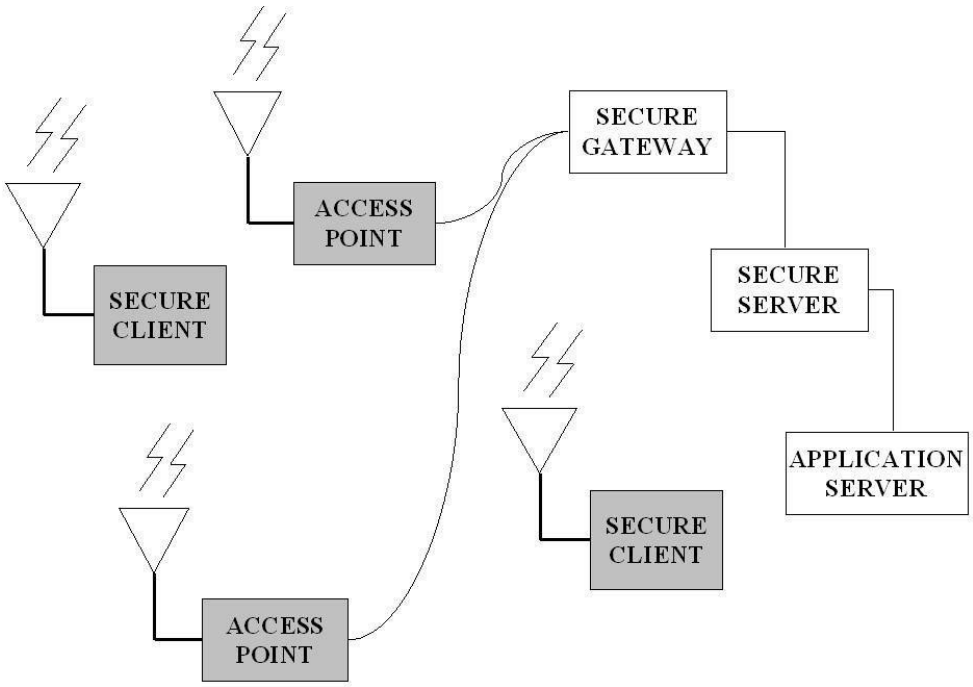


Figure 1 – Topología de una Red Cableada, también muestra posibles esquemas de seguridad.

Figura 2 – Topología para una Red Inalámbrica



G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
"2019 -Año del 25° Aniversario del reconocimiento de la autonomía de la Ciudad de Buenos Aires"

Hoja Adicional de Firmas
Anexo

Número: IF-2019-34165710-GCABA-LOTBA

Buenos Aires, Lunes 4 de Noviembre de 2019

Referencia: Buenas Prácticas de Seguridad Informática y Sistemas de Monitoreo y Video Vigilancia

---

El documento fue importado por el sistema GEDO con un total de 54 pagina/s.

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.11.04 15:30:04 -03'00'

Cattadori Federico
Subgerente
LOTERIA DE LA CIUDAD DE BUENOS AIRES S.E.
MINISTERIO DE ECONOMIA Y FINANZAS

Digitally signed by Comunicaciones Oficiales
DN: cn=Comunicaciones Oficiales
Date: 2019.11.04 15:30:05 -03'00'