PGISI-03	Todos los empleados, proveedores, contratistas y terceras personas de la LOTENAL que detecten un incidente o una debilidad a un activo, deben reportar el incidente de seguridad, a través de los lineamientos definidos por las Gerencias de la Dirección de Informática y la Gerencia de Servicios Generales, dependiendo de si se trata de información, hardware, software, recursos humanos, inmuebles o algún otro tipo de activo. A.16.1.2 y 16.1.3 y 6.1.4
PGISI-04	Todos los empleados, proveedores, contratistas y terceras personas deben apegarse a lo que especifique la Dirección de Informática y la Gerencia de Servicios Generales para el seguimiento y respuesta de los Incidentes de Seguridad de acuerdo a su tramo de control. A.16.1.5
PGISI-05	Las Gerencias de la Dirección de Informática deben registrar la solución de todos los incidentes de seguridad que son de su competencia, aportando evidencia con el fin de contar con una base de conocimientos de dichos incidentes. A.16.1.6
PGISI-06	Las Gerencias de la Dirección de Informática y la Gerencia de Servicios Generales deben resguardar en lugares seguros todo el seguimiento y evidencia que se genere para la conclusión de los incidentes de seguridad, ya que pueden servir de evidencia para cualquier cuestionamiento que se presente. A.16.1.7

POLÍTICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

OBJETIVO

Establecer políticas para la administración de aspectos de seguridad de la información para la gestión de la continuidad del negocio.

Las aplicaciones de los siguientes controles pertenecen al **"Anexo A",** de la norma ISO/IEC 27001:2013.

- **A.17.1 Continuidad de la seguridad de la información**
  - A.17.1.1 Planificación de la continuidad de la Seguridad de la Información
  - A.17.1.2 Implementar la continuidad de la Seguridad de la Información
  - A.17.1.3 Verificación, revisión y evaluación de la continuidad de la Seguridad de la Información
- **A.17.2 Redundancias**
  - A.17.2.1 Disponibilidad de los recursos de tratamiento de la Información.

NOMENCLATURA

Para distinción de las políticas expresadas en este documento con otras que se hayan establecido, se realizará de la siguiente manera:

- **PASIGCN**, representa que la política mencionada pertenece al título de la misma.
- Los últimos dígitos representan el consecutivo de las políticas expresadas.

POLÍTICAS

PASIGCN-01	Cada Gerencia al alcance de la certificación debe definir, determinar y documentar si le aplica un plan de contingencia para continuar con la operación en caso de situaciones adversas, como una crisis o desastre. A.17.1.1
PASIGCN-02	Las Gerencias que tengan planes de contingencia deben de establecer, documentar, implementar y mantener procedimientos para la continuidad del negocio. A.17.1.2

PASIGCN-03	Las Gerencias que en su plan de contingencia involucren a proveedores, contratistas y terceras personas, para su ejecución deben considerar al menos la utilización de contratos, convenios y acuerdos recíprocos. A.17.1.2
PASIGCN-04	Las Gerencias que tengan planes de contingencia deben ejecutarlo mínimo una vez al año para evaluar su efectividad y mejoras. A.17.1.3
PASIGCN-05	La Gerencia de Telecomunicaciones y de Centro de Cómputo, deben implementar la redundancia requerida para los aplicativos, las comunicaciones de red voz y datos en alta disponibilidad con el fin de mantener la operación sustantiva de la LOTENAL en continua funcionalidad. A.17.2.1

POLÍTICAS DE RELACIÓN CON PROVEEDORES

OBJETIVO

Evitar incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales.

Las aplicaciones de los siguientes controles pertenecen al **"Anexo A",** de la norma ISO/IEC 27001:2013.

- **A.18.1 Cumplimiento de los requisitos legales y contractuales**
  - A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
  - A.18.1.2 Derechos de propiedad intelectual (DPI)
  - A.18.1.3 Protección de los registros de la organización
  - A.18.1.4 Protección y privacidad de la información de carácter personal
  - A.18.1.5 Regulación de los controles criptográficos
- **A.18.2 Revisiones de la seguridad de la información**
  - A.18.2.1 Revisión independiente de la seguridad de la información
  - A.18.2.2 Cumplimiento de las políticas y normas de seguridad
  - A.18.2.3 Comprobación del cumplimiento técnico.

NOMENCLATURA

Para distinción de las políticas expresadas en este documento con otras que se hayan establecido, se realizará de la siguiente manera:

- **PCRL**, representa que la política mencionada pertenece al título de la misma.
- Los últimos dígitos representan el consecutivo de las políticas expresadas.

POLÍTICAS

PCRL-01	Las Gerencias al alcance de la certificación deben identificar y documentar las leyes, requisitos legales, regulatorios, estatutarios o contractuales que les aplica, así como el objetivo y función de la LOTENAL. A.18.1.1
PCRL-02	Se deben llevar a cabo las acciones conducentes para proteger los Derechos de Propiedad Intelectual de los productos que los proveedores desarrollen bajo el objeto de un contrato celebrado con la LOTENAL. A.18.1.2

PCRL-03	Todos los empleados, proveedores, contratistas y terceras personas deben conceder los derechos de propiedad a la LOTENAL, del diseño, construcción y prueba de sistemas, procesos, procedimientos, patentes, inventos u otros derechos de propiedad intelectual que originen y/o desarrollen bajo el alcance para el que fueron contratados. A.18.1.2
PCRL-04	La Gerencia de Nuevos Productos solicita a la Gerencia Consultiva, realice el registro de los Derechos de Propiedad Intelectual de los sorteos y nuevos productos para su protección, ante el Instituto Mexicano de Propiedad Industrial (IMPI). A.18.1.2
PCRL-05	Todas las Gerencias al alcance de la certificación que manejen información sustantiva ya sea en documentos físicos, o en medios electrónicos, deben Gestionar contra pérdida, destrucción, falsificación, revelación o acceso no autorizados en apego a los requisitos legales, regulatorios y contractuales de la LOTENAL. A.18.1.3
PCRL-06	Todos los empleados, proveedores, contratistas y terceras personas deben apegarse a la.- Ley Federal de Transparencia y Acceso a la Información Pública, Ley General de Transparencia y Acceso a la Información Pública, Ley Federal de Protección de Datos Personales en Posesión de los Particulares y Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, con el fin de no divulgar información del personal, empleados, contratistas y terceras personas en poder de la LOTENAL. A.18.1.4
PCRL-07	En caso de ser necesario, se deben implementar las leyes y regulaciones pertinentes para los controles criptográficos. A.18.1.5
PCRL-08	Las Gerencias al alcance de la certificación deben de realizar una revisión independiente, considerando Auditorías Externas a intervalos planificados o siempre que se produzcan cambios significativos en la operación de la LOTENAL, para asegurar la implantación y el buen funcionamiento de

	objetivos de control, políticas, procesos y procedimientos para la seguridad de la información. A.18.2.1
PCRL-09	Las Gerencias dentro del alcance de la certificación deben realizar un monitoreo de los controles y procedimientos que son aplicables a su tramo de control en concordancia con los dueños de los activos del SGSI. A.18.2.2
PCRL-10	La Gerencia de Sistemas Sustantivos, debe hacer uso de las mejores prácticas o metodologías para el Desarrollo de Sistemas buscando los niveles adecuados de Disponibilidad, Integridad, Confidencialidad e Interoperabilidad. A.18.2.3

GERENCIAS CRÍTICAS RESTRINGIDAS

GERENCIA	ÁREA RESTRINGIDA	FIRMA DE ACEPTACIÓN DEL GERENTE
1. Subdirección General de Finanzas y Sistemas/Dirección de Informática/Gerencia de Centro de Cómputo.	Site de centro de cómputo	Ing. Abelardo Lagunas Peñaloza Gerente de Centro de Cómputo.
2. Subdirección General de Comercialización y de Servicios/Dirección de Comercialización/Gerencia de Sorteos.	Gerencia de Sorteos	Lic. Mitzi Jocelyn Molina Ramírez Gerente de Sorteos.

NOTA.

El acceso a las áreas de infraestructuras críticas restringidas debe de ser. Soló personal autorizado y el acceso es de doble factor.

GERENCIAS RESTRINGIDAS

GERENCIA	ÁREA RESTRINGIDA	FIRMA DE ACEPTACIÓN DEL GERENTE
1. Dirección de Administración/Gerencia de Servicios Generales.	1. Cámaras de circuito cerrado. 2. Planta de emergencia. 3. Subestación eléctrica. 4. Estacionamiento de blindadas.	Lic. Alberto de la Cruz Alanís González Gerente de Servicios Generales.
2. Subdirección General de Finanzas y Sistemas/Dirección de Programación y Presupuesto/Gerencia de Crédito y Cobranza.	5. Edison 1er. Piso. Gerencia de Crédito y Cobranza.	Lic. Alejandro Roberto Pérez Pineda Gerente de Crédito y Cobranza.
3. Subdirección General de Finanzas y Sistemas/Dirección de Programación y Presupuesto/Gerencia de Tesorería	1. La bóveda.	Lic. Eric Toledo Contreras Gerente de Tesorería.
4. Subdirección General de Comercialización y de Servicios/Dirección de Comercialización/Gerencia de Ventas Área Metropolitana.	1. Almacén del departamento de distribución de expendios locales. 2. Almacén del departamento de distribución de expendedores ambulantes de billete.	Mtra. Ana Aurora Lara Martínez Gerente de Ventas Área Metropolitana.

NOTA.

Para el acceso a la Gerencia de Ventas Área Metropolitana, el registro se lleva a través de una bitácora y siempre es acompañado por una persona de la Gerencia y el acceso a las demás áreas de infraestructuras restringidas soló es personal autorizado y el acceso es de un solo factor.

COMERI
Comité de Mejora Regulatoria Interna
30 OCT 2018
APROBADO

MEDICIÓN DE LOS OBJETIVOS DEL SGSI

OBJETIVO	META PROPUESTA	INDICADOR Y/O EVIDENCIA DE CUMPLIMIENTO	GERENCIA INVOLUCRADA
Realizar la actualización de procedimientos.	Contar con la Información Documentada y Actualizada de la Operación de la LOTENAL. **Meta 50%**	(Gerencias Actualizadas / Total de Gerencias) *100. **Indicador Anual. Comenzó en diciembre de 2017**	Todas las Gerencias al Alcance del SGSI y WLA. Gerencia de Organización y Desarrollo de Personal reporta el indicador.
Gestionar e implementar la continuidad del negocio.	Asegurar que todos los procesos de negocio críticos estarán disponibles para los clientes, proveedores, y otras entidades que deben acceder a ellos. **Meta 70%**	(Planes de Contingencia Ejecutados/ Total de Planes de Contingencia) *100. **Indicador Anual. Comenzó en diciembre de 2017**	1. Centro de Cómputo 2. Telecomunicaciones 3. Servicios Generales 4. Tesorería 5. Sorteos 6. Producción 7. Crédito y Cobranza Administrador del SGSI reportará el indicador.
Trabajar con un Estándar reconocido a nivel mundial que permita reforzar la imagen, confianza y credibilidad de la LOTENAL.	Continuar manteniendo la imagen, confianza y credibilidad de la LOTENAL. **Meta 100%**	(Total de Certificaciones / Certificaciones Refrendadas) *100 **Indicador Anual. Comenzó en diciembre de 2017**	Todas las Gerencias al Alcance del SGSI y WLA. Administrador del SGSI reportará el indicador.
Hacer transparente la Gestión de la LOTENAL.	Destacar los principales atributos y productos de la LOTENAL para impulsar la comercialización así mismo poder cumplir con la transparencia que nos rige el INAI. **Meta. 70%.**	De acuerdo al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). **Indicador Semestral. Comenzó en diciembre de 2017**	Gerencias involucradas en el proceso del INAI y la Dirección de Evaluación de Recursos para la Asistencia Pública. Administrador del SGSI reportará el indicador.
Mantener actualizada y ejecutar una metodología de riesgos con el fin de que se minimicen los riesgos en la operación de la LOTENAL	Identificar, documentar, administrar y minimizar los activos en tratamiento de riesgos. **Meta 100%**	Actualización o Ratificación de la Metodología de Riesgos. **Indicador Anual. Comenzó en diciembre de 2017**	Todas las Gerencias al Alcance del SGSI y WLA. Administrador del SGSI reportará el indicador.

GERENCIA DE ORGANIZACION Y DESARROLLO DE PERSONAL
MANUAL ORIGINAL

LOTERÍA NACIONAL PARA LA ASISTENCIA PÚBLICA
SUBDIRECCIÓN GENERAL DE FINANZAS Y SISTEMAS

MANUAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN		
CATÁLOGO DE VULNERABILIDADES	REV. 00	LN-6100-MOP-AN-10
	30-Oct-18	Página 1 de 6

VULNERABILIDAD
Acceso a páginas web no autorizadas
Acceso no autorizado al edificio
Acceso telefónico no controlado
Accidentes causados por el hombre.
Agua Suministro
Aire Suministro
Alcance limitado
Almacenamiento de datos no estructurado.
Almacenamiento desprotegido
Archivo con virus
Archivo en blanco o incompleto
Archivo enviado a destiempo
Ataques de Ingeniería social
Ataques debidos a virus informáticos a través de archivos y software
Ausencias / insuficiencia de personal
Autoridad excesiva / control
Bloqueo del escape del fuego
Cableado / articulaciones / conexiones pobres
Cambio no controlado de usuarios de equipos portátiles / Tecnología de Información / equipos de comunicaciones.
Capacidad inadecuada
Carecer de recursos, recursos inadecuados, recursos incompatibles
Circunstancias personales
Comunicaciones móviles
Conexión de equipos no autorizados
Contaminación atmosférica
Contraseñas, claves, certificados sin protección
Control de descargas inadecuado
Control de eliminación de la propiedad
Control de utilidades y herramientas
Control del material / archivos fuente

Control inadecuado de consumibles
Control inadecuado de los servicios prestados al exterior
Control inadecuado de visitantes.
Control inadecuado del personal de limpieza / mantenimiento
Control insuficiente de contratistas
Copia de seguridad de datos.
Corrupción
Cuentas sin contraseña o contraseñas débiles
Cuña que estorbe en las puertas de fuego / bloqueo de las cerraduras
Daño líneas.
Daño causado por el hombre
Datos almacenados en PABX
Deficiente el desarrollo del sistema
Degradación
Derechos de autor / I.P.R.
Desastre causado por el hombre.
Desastre natural
Descuido del cajero
Desgaste causado por el hombre
Desgaste en el uso
Desgaste en la cabeza magnética
Desmantelamiento de partes del equipo como: Teclado, monitor, mause, disco duro entre otro.
Detección inadecuada de prevención de incendios / detección
Discos compactos de auto - inicio
Disponibilidad de la red de topografía
Disponibilidad de servicios de topografía
Efectos nocivos para el medio ambiente - sistema de calefacción, humedad, ruidos, luz, olor, etc.
Ejecución remota de código
El sistema no cumple con lo necesario para la operación
Eliminación de equipos para mantenimiento
Eliminación y reutilización de medios de almacenamiento.
Empleado disgustado.
Enfoque de competidor.
Enfoque de los medios de comunicación
Enrutamiento de cables
Entrega desfasada u omisión del reporte
Entrega incompleta del producto o servicio
Entrega tardía del producto o servicio
Equipo de Cómputo no prende

Exclusión / inclusión en las listas de distribución de documentos
Extinguidor vacío
Extravió
Falla eléctrica
Falla en el sistema
Falla en los servidores
Fallos de seguridad de los servicios y protocolos de los cuales se permita el tráfico
Falta de bitácoras
Falta de capacitación laboral
Falta de conciencia de los fabricantes de actualizaciones
Falta de conciencia sobre la seguridad
Falta de delegación / distribución / planificación de la sucesión
Falta de documentación
Falta de entrega del producto o servicio
Falta de Equipo Auxiliar (Mantenimientos Aire Acondicionado, UPS, Sistema Contra Incendio y Planta de Emergencia)
Falta de formación específica para tele trabajadores
Falta de identificación del remitente / receptor
Falta de mantenimiento a la infraestructura
Falta de mantenimiento en el sistema
Falta de mecanismos de vigilancia
Falta de personal para dar apoyo al mantenimiento y seguimiento al Sistema de Gestión de Seguridad de la Información SGSI ISO/IEC 27001:2013 y del estándar de la Asociación Mundial de Loterías WLA SCS:2012
Falta de plan de mantenimiento
Falta de políticas / estándares / procedimientos
Falta de privilegios en el sistema
Falta de protección contra virus y código malicioso
Falta de señalamientos
Falta de validación
Falta del recurso humano para la continuidad de las operaciones de la Gerencia
Firewall débil
Formato llenado sin la descripción adecuada
Formato sin formalizar
Fraude en el pago de premios
Fuga de información a través de conexiones de tipo "sesión nula"
Gas Suministro
Gran número de puertos abiertos
Hacker
Horas de trabajo incompatibles
Impacto e interferencia electromagnética

Inadecuada / complicada interfaz de usuario
Inadecuada / incompleta especificación
Inadecuada actualización del software
Inadecuada aplicación de la regla de diseño
Inadecuada definición del puesto de trabajo.
Inadecuada protección de accesos publico
Inadecuada protección del trafico sensible
Inadecuada protección física edificio
Inadecuada protección física habitación
Inadecuada protección física del site
Inadecuado / almacenamiento
Inadecuado / insuficiente / control de configuración
inadecuado / pruebas insuficientes
Inadecuado / Uso no controlado
Inadecuado control de acceso habitación
Inadecuado control de acceso site
Inadecuado control de base de datos
Inadecuado control de la contratación
Inadecuado control de versión.
Inadecuado manejo de la configuración.
Inadecuado monitoreo y entrega del servicio
Incompatibilidad
inestabilidad en el suministro de energía eléctrica
Instalación de servicios innecesarios
Instalación de Software no autorizado
Instalaciones por defecto de sistemas y aplicaciones
Insuficiencia de controles de trabajo
Insuficiencia de la prueba de envío / recepción
insuficiencia de personal
Insuficiencia en la capacidad de la red.
insuficiencia en la clasificación de activos
Insuficiencia en la gestión de la red.
Insuficiente control de las interfaces dentro de la organización
Insuficiente filtrado de los paquetes con direcciones de inicio y destino inadecuadas
Insuficiente seguimiento de las medidas de seguridad para el medio ambiente y las infraestructuras
Interferencias provocadas por algunos dispositivos inalámbricos
La disponibilidad de copias de seguridad de los datos.
La falta de procedimiento de disposición
La inclusión de código durante la fase de diseño, no cubiertos por la especificación.

Ley de protección de datos
Licencia caduca
Licencia de Software
Líneas de comunicación no protegidas
Los datos, registros, historia, archivos temporales no se elimina de los discos duros locales
Lotes de almacenamiento volátil / material inflamable
Mal funcionamiento del POP3 y SMTP
Mal uso del correo electrónico
Mala administración de contraseñas
Mala Administración de puertos en servidor
Mala aplicación del sistema
Mala configuración en el servidor
Mala realización en el pago de Premios
Manejo inadecuado de encriptación
Negligencia del usuario al equipo PC
No contar con el capital para la contratación del proveedor
No contar con los servicios del proveedor
No contar con no break
No controlados instalación / desinstalación
No cumplir en tiempo y forma con los servicios de la Gerencia
No hay sistema disponible
No hay una política clara de escritorio.
No hay una política clara de/para pantalla.
No se encuentra actualizado
No se entrega/genera la información.
No se puede abrir el sistema
No se pueden imprimir reportes del sistema
No se tiene capacitación del sistema
No se tienen las Herramientas funcionando correctamente para la ejecución del sistema (Teclado o Mouse o Monitor)
Perdida de archivos a través del FTP (Protocolo de transferencia de archivos)
Perdida de información
Pérdida del control del DNS
Problemas de seguridad (si no poseen una buena configuración)
Problemas usuarios
Programas CGI vulnerables
Prohibición que los traidores o espías corporativos copien datos sensibles en medios físicos de almacenamiento (diskettes, memorias, etc.) y sustraigan éstas del edificio
Protección inadecuada de un cambio no autorizado.
Prueba de carga y estrés

Publicar Información inconsistente al sitio
Punto de acceso sin protección.
Registro de eventos (logging) incompleto o inexistente
Reporte con errores
Revocación de los derechos de acceso
Robo de información de archivos confidenciales
Robo, documentación incompleta del vehículo
Robos, tener adeudos
Rotura de lámpara
Rotura de mica
Servicios no deseados, como Telnet, DHCP o DNS
Sin línea.
Sincronización de tiempo
Siniestro en transito
Siniestro-Robo
Site Scrip
Sólo copia.
SQL
Suministro eléctrico
Susceptibilidad de daños a los medios de almacenamiento
Tener adeudo con la LOTENAL
Transferencia de contraseñas / claves en texto plano
Ubicación - almacenamiento desprotegido
Ubicación - exposición - contaminación
Ubicación - exposición - temperatura
Ubicación - exposición humedad / agua
Ubicación - exposición a daños
Ubicación - exposición visual, sonora o interceptación electromagnética
Ubicación del sitio
Uso de los datos de producción para fines de ensayo.
Uso de parches de software
Uso inadecuado por parte del personal
Uso incontrolado
Velocidad de transmisión limitada
Ventas bajas
Vulnerabilidades en el formato de cadenas
Y2K cumplimiento

LOTERÍA NACIONAL PARA LA ASISTENCIA PÚBLICA
SUBDIRECCIÓN GENERAL DE FINANZAS Y SISTEMAS

AMENAZA
Abuso de los derechos del administrador
Abuso de los derechos del usuario
Acceso / copias no autorizado de comunicaciones recibidas
Acceso a DNS restringido
Acceso a IP restringida
Acceso a la red de usuarios no autorizados
Acceso a los sistemas y documentos al personal de mantenimiento y de limpieza
Acceso no autorizado a la habitación
Acceso no autorizado al edificio
Acceso no autorizado al site
Acceso y manipulación de información a través del web
Accesos de software malicioso por medio de soportes extraíbles, USB, DVD o CD
Accidentes de líquidos = Accidentes al equipo por líquidos o comida
Acción industrial
Amplio tiempo de respuesta a través de diferentes zonas horarias y horas de trabajo
Análisis de mensajes de flujo
Análisis de tráfico
Ancho de banda insuficiente para soportar el tráfico de consultas
Archivos ejecutables erróneos
Atacar a otra página desde el sitio
Ataque denegación del servicio
Ataque malintencionado - daño doloso / vandalismo
Ataque malintencionado - dispositivo incendiario
Ataque malintencionado - explosivos
Ataque malintencionado - intención de robo
Ataque malintencionado - la radiación electromagnética (acto de guerra
Ataque malintencionado - químico
Ataque malintencionado -acceso a los servicios de sitio
Ataque malintencionado - manipulación de datos o software
Ataque malintencionado - manipulación de equipos informáticos
Ataque malintencionado- uso de armas (acto de guerra o disturbios civiles)

Ataques de usuarios negligentes
Ataques internos dentro del perímetro de seguridad de la LOTENAL
Ataques locales o remotos (por medio del root)
Ataques remotos a la base de datos
Baja de la Institución
Baja del billetero en el padrón nacional de vendedores ambulantes de billetes
Cables de energía y del equipo de cómputo rotos
Cancelación de los derechos de acceso
Carga electrostática
Coacción a los funcionarios
Código troyano
Compromisos / chantaje de persona
Conexión de equipo no autorizado
Contingencia de la Gerencia
Control deficiente de la codificación de metodología
Copia no controlada de documentos
Correo bomba
Correo electrónico no funciona
Corrupción de datos
Crackeo
Cruce de información
Dañar componentes de la PC
Daño a las líneas
Daño accidental - [de] material de construcción
Daño accidental - aeronaves
Daño accidental - agua / suciedad
Daño accidental - colisión vehicular
Daño accidental - contaminación química
Daño accidental - daño de personal o de equipo
Daño accidental - durante la construcción y el mantenimiento
Daño accidental - falla del aire acondicionado
Daño accidental - fuego
Daño accidental - fuertes campos magnéticos
Daño accidental - temperatura extrema / humedad
Daños - animal / insecto / bacteriológicas
Debilita la imagen institucional
Degradación de disponibilidad
Degradación de documentos en papel
Degradación del tiempo de respuesta
Denegación de servicio

Desastre natural - Huracán
Desastre natural - Inundación
Desastre natural - Rayo
Desastre natural - Terremoto
Descarga eléctrica
Descarga no controlada de software
Desconfiguración del equipo de cómputo
Desconfiguración del equipo de cómputo para imprimir
Desconocimiento del usuario
Descuidado en la comunicación de información a receptores no autorizados
Desvío de las comunicaciones
Desvío de recursos
Desvío de ruta de las comunicaciones
Deterioro de los soportes de almacenamiento
Deterioro del equipo
Dificultad para detectar fallos
Disminución en las ventas de billete por falta de billeteros
Disminuye una de las fortalezas de la LOTENAL detectadas en el PROGRAMA Institucional 2014-2018 de la Lotería Nacional para la Asistencia Pública
Divulgación de contraseñas
Documentos en fotocopiadora, impresora, escáner, fax
Duplicar Página
Ejecución de código ilegal a nivel servidor recuperar cualquier información deseada que esta contenga
El billetero pierde ayuda, apoyos e incentivos
El equipo de cómputo se apaga a cada rato
El personal de la Gerencia es de nuevo ingreso
El robo / pérdida de teletrabajo equipos / datos
El sistema se encuentra en mantenimiento
El uso indebido de las medidas de seguridad - "tailgating", el uso indebido de acceso ficheros, etc.
El uso no autorizado de los datos almacenados en PABX
Eliminación de algunos archivos
Eliminación de archivos de la base de datos
Eliminación no controlada de documentos
Empleado con más privilegios en el sistema de los que se requieren para su operación
Empleado corrupto
Empleado disgustado
Empleado entro al sistema con una contraseña con privilegios de administrador
Empleado no conoce cómo opera el sistema

Empleado no conoce sus funciones
Empleado sin privilegios en el sistema
Enlaces permanecen activos final de las comunicaciones a través de RDSI o conexión de módem.
Enmascaramiento de la identidad del usuario
Entrega de información a destiempo de los procesos. ASI y OPEC del Manual Administrativo de Aplicación General en las materias de tecnologías de la información y comunicaciones, y en la de seguridad de la información MAAGTICSI
Equipo de cómputo hackeado
Equipo de cómputo no prende
Equipo de cómputo sin desbloquear
Equipo de cómputo sin protección de contraseña
Equipo de cómputo tirado o mojado
Equipo en Riesgo
Error de contenido en la solicitud de publicación por parte del área solicitante
Error de publicación por parte del área de página web.
Error del personal operativo
Error en mantenimiento
Errores del usuario
Escasez de personal
Explotación de las debilidades conocidas
Exposición de contraseña
Exposición de documentos / datos
Falla del equipo de TI
Falla al encender el equipo
Falla de equipo / debido a la ambigüedad de fecha Y2K
Falla de software / corrupción
Falla en el suministro de agua
Falla en el cambio regular de contraseñas
Falla en el monitor
Falla en el respaldo de datos / documentos
Falla en el sistema de comunicaciones
Falla en el suministro de energía
Falla en el suministro de gas
Falla en el uso de medidas previstas de seguridad
Falla en la copia de seguridad de los datos
Falla en la instalación del hardware
Falla en la utilización de parches para eliminar debilidades de seguridad conocidas.
Falla en las comunicaciones de largo rango dependientes de P.T.O.
Falla en los servicios de comunicación

Falla no interpreta el contenido
Falla por no recibir información
Falla técnica en los componentes de red
Fallas en el equipo de energía de respaldo
Falta de capacidad del equipo de cómputo.
Falta de capacitación del sistema
Falta de mantenimiento al equipo de cómputo
Falta de mantenimiento al lugar de almacenamiento
Falta de pistas de auditoria
Falta de privilegios del sistema
Falta de pruebas en el sistema comprado
Falta de Red
Falta de seguridad en el sistema
Falta ejecutar el mantenimiento a los equipos de computo
Faltas repetidas e injustificadas de asistencia
Fecha del servicio en destiempo
Frustración del usuario.
Hardware excedente no autorizado al equipo, como, porta lap, protector de pantalla, bocinas, audífonos, lámparas, ventiladores, entre otros
Importación y exportación ilegal de software
Impresora descompuesta
Impresora desconfigurada
Impresora sin red
Incumplimiento a lo establecido en el contrato Anexo Técnico
Incumplimiento de la legislación
Indisciplina o desobediencia en el trabajo
Infiltración en las comunicaciones
Infracción de los derechos de autor
Ingeniería social
Instalación de virus troyanos
Insuficiencia de la capacidad del sistema de comunicaciones
Intento sistemático de acceso a contraseñas
Intercepción de datos
Intercepción de líneas
Interferencia de transmisión
Interrupción del servicio durante la instalación / actualización a equipos
Inyección de código
La contaminación de polvo / polen y esporas
La tinta se acaba
Las áreas involucradas no validan la información contenida

Macro virus
Mal manejo del correo electrónico
Mal uso de la contratación
Mal uso de las herramientas de trabajo
Mala configuración del Gestor de contenidos
Mala coordinación de actividades por parte de empleados, contratistas, terceros o proveedores
Mala Optimización en el Sistema Operativo del Servidor
Manipulación de líneas
Manipulación del equipo de teletrabajo por el empleado
Manipulación del equipo de teletrabajo por un familiar / visitante
Manipulación inadvertida de datos
Modificar Página
Modificar Registros de las Tablas
Muerte o lesión de personal
Negación del servicio
Negligencia en la eliminación de datos
No abrir el expendio local
No bloquear el equipo
No contar con equipos de cómputo para el desarrollo
No cumplir con las responsabilidades y metas asignadas del empleado
No cumplir con los objetivos de la Gerencia
No cumplir en tiempo y forma los servicios de la Gerencia
No entregar devolución de billete en el horario señalado por la H. Junta Directiva.
No funciona el teclado o el mouse
No hay un control de las versiones del sistema
No hay un requerimiento formal de la compra del sistema o desarrollo
No pagar el premio
No porta la credencial institucional
No publicar oportunamente promocionales
No pueden abrir el sistema
No reconoce la contraseña
No registran adecuadamente la información
No se cuenta con excepciones para cachar el error del sistema
No se encuentra el icono de acceso en el escritorio
No se encuentra el personal que autoriza el formato
No se puede tener acceso al sistema
No se realizan los pagos en tiempo y forma
No se registran las ventas del billetero
No tener el software necesario para el desarrollo del sistema

No tener la continuidad contractual del personal de desarrollo del sistema
Obtener Información de la Base de Datos
Obtener información del sitio
Ofensas verbales o físicas a empleados, contratistas, terceros o proveedores
Omisión de las políticas del SGSI Y WLA
Oportunidad de una "puerta trasera" de acceso
Perdida de confidencialidad
Pérdida de disponibilidad para los usuarios autorizados
Perdida de Información por medio del POP3 y SMTP
Perdida de información total o parcial del disco duro
Perdida de la confianza institucional de las partes interesadas
Personal sin capacitación de los procedimientos institucionales
Picos de tensión / aumentos repentinos / fluctuaciones
Prueba incompleta improbable
Publicidad adversa sin vigilancia de los medios de comunicación 'entrevista'
Puerta abierta de la oficina y equipo de cómputo desbloqueado
Que la computadora no inicie
Que la computadora se reinicie sola
Que se abran ventanas con publicidad o pornografía
Registro de cambios o modificaciones insuficientes
Rendimiento inesperado
Repudio
Respaldos de información no disponibles
Retraso en la operación de la evaluación semestral
Robo de datos / documentos
Robo de equipo
Robo de equipo móvil
Robo de información
Robo de Información a través del FTP o correo electrónico
Robo de material consumible
Robo de Software
Sistema desactualizado
Sistema lento al mostrar la información
Sistema se bloqueó durante la operación
Sistema sin protección de contraseña
Sobre carga de servicio deliberada
Sobrecarga de trafico
Software malintencionado
Tirar el sitio
Transferencia de archivos a través del FTP

Transmisión de errores
Uso de software de manera no autorizada
Uso de software sin licencia
Uso del servicio de red no autorizado
Uso del software por usuarios no autorizados
Uso ilegal de software
Uso inadecuado de los medios de almacenamiento
Uso inapropiado del equipo de comunicación
Uso indebido de los puertos de acceso remoto para la gestión y diagnóstico
Uso indebido de servicios de correo electrónico
Uso no autorizado de los dispositivos de almacenamiento
uso no autorizado de sistemas de TI
Uso no controlado de enlaces de comunicaciones
Uso sin control de recursos
Usuario con privilegios de administrador o súper usuario
Usuario sin capacitación
Verificación difícil / imposible
Violación al acuerdo de confidencialidad
Virus de archivos
Virus en el equipo de cómputo
Virus en el sector de arranque
Visualización, copia, eliminación de archivos / documentos no autorizada