No.	Objetivo de control	Control	Aplica	Motivo
		Cada consignación de billetes debe ser formalmente comprobada a su llegada.		tener un registro para evidencia y trazabilidad.
		L.1.4.3 Procedimiento de verificación de billetes. Se debe verificar mediante un procedimiento de comprobación de entregas a su llegada, que los números de los precintos son correctos y que la seguridad del contenedor se ha preservado.	Sí	Mantener el control sobre las entregas de billetes tradicionales para evitar que se vulnere la confidencialidad y en su caso identificar cualquier situación que ponga el riesgo la entrega del billete.
		L.1.4.4 Resultado de la verificación de billetes. Los resultados de la verificación deben documentarse y en caso de no conformidades y/o irregularidades se debe actuar para determinar si se ha comprometido la seguridad de un envío.	Sí	Mantener el control documentado sobre las entregas de los billetes tradicionales, de lo contrario identificar cualquier situación de manera inmediata con la trazabilidad adecuada.
		L.1.4.5	Sí	Mantener la evidencia y trazabilidad de la distribución

No.	Objetivo de control	Control	Aplica	Motivo
		Sistema de control de billetes. Se deben contabilizar -mediante un sistema de control en funcionamiento- los paquetes de billetes desde su llegada a los almacenes de la organización hasta el momento que llegan al punto de venta.		del billete tradicional , con el fin de verificar el cumplimiento adecuado y de ser necesario ejecutar de inmediato una acción correctiva y/o preventiva según sea el caso.
L1.5	Seguridad en los puntos de venta (comisionistas) lotería instantánea	L.1.5.1 Recepción de billetes en los puntos de venta. La organización debe requerir a los comisionistas, bien por vía contractual o por los medios que corresponda, que validen la integridad de los paquetes de billetes al momento de la recepción. Asimismo, se les debe solicitar que confirmen la recepción concreta de cada una consignación de billetes.	Sí	Confirmar que los billetes tradicionales llegaron íntegros con los organismos de venta.
		L.1.5.2	Sí	Mantener la evidencia de que los billetes tradicionales llegaron íntegros y sin

No.	Objetivo de control	Control	Aplica	Motivo
		Confirmación de recepción. Tan pronto se disponga de la confirmación de recepción, se debe registrar formalmente que los billetes se han emitido a ese punto de venta.		contratiempos al punto de venta.
		L.1.5.3 Instrucciones para los minoristas. La organización debe dar instrucciones a los comisionistas sobre pago de premios, validación de billetes, manejo y almacenamiento de billetes, comunicación de asuntos de seguridad y la gestión de billetes perdidos y robados.	Sí	Que los organismos de venta tengan todo el conocimiento sobre el manejo de los billetes tradicionales, así como alguna contingencia que se llegue a dar.
		L.1.5.4 Capacitación de los minoristas en materia de seguridad. La organización debe proporcionar y documentar la capacitación a	Sí	Que los organismos de venta, cuenten con los lineamientos necesarios en seguridad para la venta de billete.

No.	Objetivo de control	Control	Aplica	Motivo
		comisionistas que les permita cumplir con los requisitos de seguridad asociados al manejo de billetes de lotería instantánea.		
L1.6	Cierre de juegos de lotería instantánea.	L.1.6.1 Procedimiento de cierre del juego. La organización debe establecer el procedimiento a ser empleado para el cierre del juego.	Sí	Que exista la determinación en los cierres del sorteo de la LOTENAL, tanto de acciones, como de responsables, roles y responsabilidades.
		L.1.6.2 Información para los minoristas. Debe establecerse y documentar el método y calendario para informar a los comisionistas sobre el cierre de un juego y la recolección de billetes.	Sí	Contar con un procedimiento que indique sin duda alguna al organismo de venta, acerca de los calendarios de sorteos tradicionales y cierre de los mismos.
		L.1.6.3 Cuadre de inventario y existencia de billetes.	No	La LOTENAL, no aplica esta operación en el billete tradicional.

No.	Objetivo de control	Control	Aplica	Motivo
		Debe establecerse el método de cuadre entre inventario y existencia de billetes de juego en la LOTENAL que se encuentran en almacenes y en puntos de venta.		
		L.1.6.4 Auditorías de comprobación de existencia (Control de inventario). Deben establecerse documentalmente los requisitos de auditorías de comprobación de existencia de billetes.	No	La LOTENAL, no aplica esta operación en el billete tradicional.
		L.1.6.5 Personal autorizado. Se debe definir formalmente quienes están autorizados para cerrar un juego y/o a destruir billetes.	Sí	Determinar roles específicos que permitan que se lleve a cabo de manera estructurada y segura el cierre de un sorteo y la destrucción de billetes tradicionales.
		L.1.6.6 Destrucción de billetes. Debe estar formalmente establecido el método y	Sí	Contar con un proceso que permita sólo la destrucción de billetes tradicionales que se deben destruir.

No.	Objetivo de control	Control	Aplica	Motivo
		forma de control de la destrucción de billetes.		
L2	Sorteos de Lotería.	L.2.1.1 Acto del sorteo. Debe estar establecida una política que asegure que los actos de sorteo de lotería se desarrollan como actos planificados y controlados, conforme a instrucciones de trabajo claras.	Sí	Para que los sorteos de la LOTENAL, se realicen en tiempo y forma.
		L.2.1.2 Instrucciones para la celebración del sorteo. Antes de cada sorteo la organización debe haber publicado las instrucciones de trabajo incluyendo instrucciones especiales con respecto al sorteo.	Sí	Tener roles definidos en cada sorteo, con el fin de que se realicen en tiempo y forma.
		L.2.1.3 Miembros del equipo de sorteo. Las instrucciones de trabajo deben incluir la composición (personas) del equipo de sorteo	Sí	Tener la certeza de que se tiene el conocimiento de las partes que intervienen, sus obligaciones y roles para la preparación de los sorteos, además de asegurar la continuidad de la operatividad al tener los datos de contacto de los mismos.

No.	Objetivo de control	Control	Aplica	Motivo
		incluyendo sus números de teléfono de contacto.		
		L.2.1.4 Deberes del equipo de sorteo. Las instrucciones de trabajo deben incluir las responsabilidades de los miembros identificados del equipo de sorteo.	Sí	Tener la certeza de que se tiene el conocimiento de las partes involucradas acerca de las obligaciones y roles de las personas que participan en los sorteos.
		L.2.1.5 Equipo de sorteo de reserva. Las instrucciones de trabajo deben nombrar e identificar a las personas de reserva y dar detalles sobre el despliegue del equipo de reserva.	Sí	Contar con un registro actualizado del equipo que podrá cubrir las posiciones de responsabilidad del personal, en caso de que por algún motivo este no pueda cumplir con las actividades del sorteo.
		L.2.1.6 Horario y la cronología del sorteo. Las instrucciones de trabajo deben incluir los horarios y la cronología detalladas de las operaciones del sorteo desde la apertura del	Sí	Para que cualquier persona que se integre a la Gerencia de Sorteos, y lea los procedimientos sepa cuál es su participación y responsabilidad en el sorteo.

No.	Objetivo de control	Control	Aplica	Motivo
		recinto del sorteo hasta el cierre del mismo.		
		L.2.1.7 Observadores del sorteo. Las instrucciones de trabajo deben incluir detalles de cualquier requisito relativo a las normas sobre la operación de la lotería sobre la obligación de presencia de observadores independientes durante el sorteo.	Sí	Mantener documentada la presencia de los integrantes del presídium que presencian la celebración del sorteo.
L2.2	Celebración del sorteo.	L.2.2.1 Procedimiento del sorteo. La organización debe establecer un procedimiento de sorteo detallado que asegure que todas las funciones que se ejecutan de manera conforme con las reglas aplicables del juego de lotería y con los requisitos regulatorios.	Sí	Identificar, documentar y actualizar todas las funciones y operaciones del sorteo.
		L.2.2.2	Sí	Identificar, documentar y actualizar todas las funciones y operaciones del sorteo.

No.	Objetivo de control	Control	Aplica	Motivo
		Guía del sorteo paso a paso. El procedimiento de sorteo debe incluir una guía paso a paso del proceso del sorteo.		
		L.2.2.3 Lugar del sorteo. El procedimiento del sorteo debe definir el lugar de celebración del sorteo.	Sí	Identificar, documentar y actualizar todas las funciones y operaciones, del sorteo.
		L.2.2.4 Asistencia al sorteo y responsabilidades. El procedimiento de sorteo debe definir quiénes asisten al sorteo y cuáles son las responsabilidades y acciones de todos los participantes.	Sí	Identificar, documentar y actualizar todas las funciones, operaciones así como sus roles y responsabilidades de cada persona que participa en el sorteo.
		L.2.2.5 Supervisión del sorteo.	Sí	Con el fin de que la celebración del sorteo sea lo más transparente para los clientes, al contar con auditores e interventores;

No.	Objetivo de control	Control	Aplica	Motivo
		El procedimiento de sorteo debe definir la política respecto a la asistencia de un "oficial de cumplimiento" (independiente) o un auditor.		
		L.2.2.6 Seguridad de las actividades del sorteo. El procedimiento de sorteo debe incluir medidas de seguridad adecuadas para las actividades del sorteo y para todo el equipamiento utilizado durante el mismo.	Sí	Identificar, documentar y actualizar todas las funciones, operaciones, así como la seguridad y el equipo qué se requiere en el sorteo.
		L.2.2.7 Emergencias durante el sorteo. El procedimiento de sorteo debe incluir las acciones a tomar en caso de que suceda una emergencia durante la celebración del sorteo.	Sí	Contar con medidas de prevención y contingencia, con el fin de garantizar la continuidad de negocio en la celebración de sorteos.
L2.3	Equipamiento del sorteo y conjuntos de bolas.	L.2.3.1 Procedimiento de inspección.	Sí	Contar con la revisión y en su caso mantenimiento periódico del instrumental y materiales que son utilizados en la elaboración del sorteo que

No.	Objetivo de control	Control	Aplica	Motivo
		Debe estar en vigor un procedimiento para la inspección de forma periódica del equipamiento de sorteo y los conjuntos de bolas, al momento de su entrega por parte del fabricante y a partir de entonces, tras consultar con una autoridad independiente. Ello con el fin de asegurar el cumplimiento con las especificaciones técnicas y los estándares.		permitan que las calibraciones y estándares requeridos para que la celebración del sorteo se cumpla.
		L.2.3.2 Inspecciones periódicas y mantenimiento. Deben realizarse, al menos anualmente, inspecciones y mantenimiento del equipamiento de sorteo, y documentarse, para cumplir a lo largo de la vida útil del equipamiento las condiciones de operación especificadas.	Sí	Contar con la revisión y en su caso mantenimiento periódico del material y equipo que son utilizados en la elaboración del sorteo que permitan los estándares requeridos para que la celebración del mismo se cumpla.
		L.2.3.3 Conjuntos de bolas compatibles.	Sí	Asegurarse que el peso y las medidas de las bolas, tengan el

No.	Objetivo de control	Control	Aplica	Motivo
		La organización debe tener en vigor un procedimiento que estipule el uso de conjuntos de bolas fabricados, con las medidas y peso, y sus tolerancias compatibles con el equipamiento de sorteo (bombo) que se emplea.		tamaño y peso requeridos para la celebración del sorteo.
		L.2.3.4 Equipamiento alternativo (de remplazo) del sorteo. La organización debe tener en vigor, si el sorteo es transmitido en vivo, un procedimiento que estipule la disponibilidad de equipamiento de sorteo alternativo y uno o varios conjuntos de bolas alternativos para su empleo en caso de problemas mecánicos o fallas de cualquier tipo.	Sí	Contar con un equipo completo para celebración de sorteos en caso de contingencias, para garantizar la continuidad de negocio en la celebración de sorteos.
		L.2.3.5 Manejo, almacenamiento y traslado del	Sí	Que las bolas que se ocupan en la celebración del sorteo, siempre se encuentren en las mejores condiciones físicas y de seguridad.

No.	Objetivo de control	Control	Aplica	Motivo
		equipamiento del sorteo y conjunto de bolas. La organización debe tener en vigor un procedimiento que estipule el almacenamiento, traslado y manejo seguro del equipamiento de sorteo y conjuntos de bolas.		
L.2.4	Sorteos Electrónicos.	L.2.4.1 Protección técnica del sistema, físico y lógico. Tomar medidas para garantizar que solo personal autorizado tenga acceso al desarrollo lógico de números aleatorios o al algoritmo, para evitar cualquier modificación al código fuente y estar protegidos contra robos, modificaciones no autorizadas e interferencias, en el sistema.	No	La LOTENAL no celebra sorteos electrónicos.

No.	Objetivo de control	Control	Aplica	Motivo
		L.2.4.2 Transacciones seguras. Tomar medidas para garantizar la integridad y autenticidad de los datos transmitidos entre el RNG (código fuente) y el algoritmo.	No	La LOTENAL no celebra sorteos electrónicos.
		L.2.4.3 Aleatoriedad, integridad y verificación del sorteo electrónico. Antes del despliegue del sistema, deben ser realizadas pruebas por partes independientes, para verificar que el sistema electrónico es aleatorio. La organización debe documentar una política relacionada con las pruebas posteriores al despliegue para verificar que el generador de números aleatorios y el algoritmo están funcionando como se lo especifican.	No	La LOTENAL no celebra sorteos electrónicos.
		L.2.4.4 Separación de tareas.	No	La LOTENAL no celebra sorteos electrónicos.

No.	Objetivo de control	Control	Aplica	Motivo
		Se debe implementar un procedimiento específico relacionado con la separación de funciones involucradas en el sorteo electrónico, para evitar cualquier fraude interno. Ninguna persona se le debe permitir realizar más de uno de los siguientes tipos de tareas: mantenimiento, monitoreo o realización de sorteos en equipos de juegos electrónicos.		
L3	Seguridad en los puntos de venta.	L.3.1.1 Contrato del punto de venta. La relación con los comisionistas debe estar sujeta a los términos de un contrato establecido.	Sí	Asegurar que los organismos de venta cumplan los requisitos que solicita la LOTENAL.
		L.3.2.1 Seguridad del punto de venta. La organización debe especificar los requisitos de seguridad que el punto de venta debe cumplir. Ello hará posible que el punto de venta se adecue y esté	No	No aplica la seguridad del punto de venta en la LOTENAL, toda vez que, en la **LEY ORGÁNICA DE LA LOTERÍA NACIONAL PARA LA ASISTENCIA PÚBLICA**, Artículo 11 párrafo II, que a la letra dice. "**La propiedad de los billetes corresponderá a la Lotería Nacional para la Asistencia Pública, mientras no se enajenen a terceros. Sin embargo, los referidos**

No.	Objetivo de control	Control	Aplica	Motivo
		conforme con los requisitos de la organización en materia de seguridad.		**expendedores y vendedores se convertirán automáticamente en propietarios de los billetes que no logren enajenar, y cuya devolución al organismo no la efectúen dentro del plazo y forma que, con carácter general, establezca la Junta Directiva".**
		L.3.3.1 Seguridad de las transacciones. Los terminales de juego deben incluir prestaciones que permitan la autenticación y cifrado del tráfico de datos entre el terminal y los sistemas de juego centrales.	No	La Entidad no cuenta con terminales de Juego.
		L.3.3.2 Pruebas de seguridad de terminales. Previo a su uso en el entorno de producción, se debe completar un concienzudo programa de pruebas relativo a las funcionalidades de seguridad de terminal. Estas pruebas deben incluir comprobaciones	No	La Entidad no cuenta con terminales de Juego.

No.	Objetivo de control	Control	Aplica	Motivo
		de que este instalada la versión correcta de la aplicación software.		
		L.3.3.3 Seguridad de terminales de autoservicio. Las terminales de autoservicio deben disponer de mecanismos de seguridad que protejan la integridad del juego.	No	La Entidad no cuenta con terminales de Juego.
L4	Custodia del dinero de premios.	L.4.1.1 Validez de la información de premiados. En relación con los premiados, la organización debe implementar procedimientos que aseguren la validez de las transacciones, de los billetes/resguardos y de las solicitudes de cobro.	Sí	Es que la LOTENAL, cuente con procedimientos y operaciones seguras, para el cobro de billetes.
		L.4.1.2 Procesos de validación. La organización debe definir y documentar los procesos de validación	Sí	Es que se cuente con la documentación necesaria para que los ganadores puedan consultar la forma y los niveles de pago de premios en la LOTENAL.

No.	Objetivo de control	Control	Aplica	Motivo
		para los distintos niveles de premio y tipos de juegos.		
		L.4.1.3 Pago de premios. La organización debe establecer un proceso para el pago o transferencia del dinero de premios.	Sí	Mantener la integridad y confidencialidad de las transacciones que se generen al ganar un premio.
		L.4.2.1 Número único de referencia del billete/resguardo. El sistema central de juegos en línea en producción debe poder incluir en cada billete/resguardo un número de referencia único.	Sí	Para tener el control y trazabilidad del billete que se comercializa, desde que está a la venta hasta el pago de premio, en caso de ser ganador.
		L.4.2.2 Procedimiento para la protección del dinero de premios pendientes de pago. La organización debe establecer un procedimiento específicamente referido	Sí	Mantener de manera segura el manejo de los datos relacionados con los premios de los sorteos, así como los no solicitados.

No.-	Objetivo de control	Control	Aplica	Motivo
		a la protección del dinero de premios pendientes de pago y de los archivos de datos que contengan información sobre la situación de pago de premios de cada juego, las transacciones específicas que están pendientes y los archivos de validación.		
		L.4.2.3 Período de pago de premios y auditoría. El procedimiento debe incluir el período completo de pago de premios, así como la auditoria de las transferencias de liquidación final del juego.	Sí	Tener documentado la vigencia de premios, tanto internamente como externamente.
		L.4.2.4 Reglas de pago e investigaciones. El procedimiento debe confirmar las reglas sobre el período de validez del billete/resguardo (caducidad), pago de	Sí	Contar con un documento en el que se pueda tener una metodología, del pago de premios en el que se pueda confirmar la validez, en cuestión de caducidad y/o rotos o maltratados.

No.	Objetivo de control	Control	Aplica	Motivo
		premios de billetes/resguardos perdidos o en mal estado, investigaciones específicas sobre la validez de solicitudes de cobro de premios y cobro de premios tardíos o de último minuto.		
		L.4.2.5 Control de acceso a la información sobre premios pendientes de pago. El procedimiento debe confirmar que el control de acceso es estricto y limitado a lo necesario para los registros relativos a premios pendientes de pago.	Sí	Evitar fuga de Información y garantizar la seguridad y la integridad de la información en el sistema, así como, en las Bases de Datos.
		L.4.2.6 Notificación de accesos. El procedimiento debe confirmar que existe un proceso de notificación (alerta) en el caso de que se produzca algún intento de acceso no autorizado.	Sí	Controlar y administrar los intentos de acceso no autorizados, a los sistemas sustantivos de la Entidad.

No.	Objetivo de control	Control	Aplica	Motivo
		L.4.2.7 Proceso de escalado. El procedimiento debe confirmar que existe un proceso de escalado de cualquier incidente actividad sospechosa.	Sí	Gestionar si el intento de acceso no autorizado, se ve en un nivel más alto.
		L.4.2.8 Auditoría de información de registro de acceso. El procedimiento debe confirmar que el dinero de premios pendientes de pago está resguardado.	Sí	Contar siempre con la liquidez necesaria para el pago de premios.
		L.4.2.9 Trazas de auditoría. El procedimiento debe confirmar que se mantienen trazas de auditoría que permiten identificar patrones no habituales de pagos tardíos.	No	No aplica toda vez que el billete se paga de acuerdo a los lineamientos de la LOTENAL.
L5	Personal de Ventas y Servicios al Cliente.	L.5.1.1 Personal que trabaja fuera de las instalaciones de la organización.	Sí	Salvaguardar la integridad física del personal que se va a los sorteos foráneos, tomando las medidas adecuadas de protección.

No.	Objetivo de control	Control	Aplica	Motivo
		Debe estar en vigor una política que asegure que el personal que trabaja fuera de las instalaciones de la LOTENAL recibe e implementa un adecuado nivel de protección.		
		L.5.2.1 Personal que trabaja en áreas críticas con acceso del público. Debe estar en vigor una política que asegure que el personal que trabaja en áreas críticas de acceso del público recibe un adecuado nivel de protección.	Sí	Asegurar un óptimo nivel de seguridad para el personal que mantiene trato directo con el público.
L6	Ventas a través de Internet y servicios interactivos.	L.6.1.1 Arquitectura de sistemas en capas. La organización debe seguir un enfoque de arquitectura de los sistemas de juego a través de Internet basado en capas, a fin de asegurar el	No	La LOTENAL no tiene ventas a través de Internet, sólo tiene canales de venta y se realiza a través de un contrato, con los Organismos de Venta.

No.	Objetivo de control	Control	Aplica	Motivo
		almacenamiento y procesado seguro de la información.		
		L.6.1.2 Ataques activos y pasivos. Deben estar desplegadas las medidas apropiadas para minimizar el éxito y/o el impacto de ataques activos y pasivos típicos.	Sí	Que la información de la Entidad se mantenga lo más integra y disponible para las áreas a través de Firewalls y controles de acceso.
		L.6.1.3 Segregación de redes. Las bases de datos de producción que contienen datos de participantes o transacciones y el servidor Web deben estar ubicados en redes separadas.	Sí	Tener un control de las transacciones, así como de las entradas y salidas de las entidades externa de la LOTENAL, es por eso que se tiene un servidor de aplicación controlado para la operación.
		L.6.1.4 Información de sesión. Las cookies de sesión deben crearse siempre en memoria, ser aleatorias y eliminarse	No	En la página Web de la LOTENAL, no cuenta con venta a través de Internet ni servicios interactivos de juego.

No.	Objetivo de control	Control	Aplica	Motivo
		cuando la sesión de usuario termine.		
		L.6.1.5 Identificación de puntos de entrada y salida. Se deben identificar, administrar y controlar todos los puntos de entrada y salida a los sistemas de Internet.	Sí	Es contar con los niveles adecuados de seguridad, así como, administrar adecuadamente los puntos de entrada y salida, a través del Firewall y Anti spam.
		L.6.1.6 Generación y almacenamiento de logs (registros). Los logs deben generarse en cada componente sensible del sistema para ser monitoreados y rectificar anomalías, defectos y alertas. Todos los logs, se almacenarán para ser presentados como evidencia un juicio.	No	La LOTENAL, no celebra sorteos electrónicos; sin embargo, se realiza el resguardo y análisis de logs de los sistemas sustantivos.
		L.6.1.7 Pruebas de seguridad. Se deben realizar pruebas de seguridad apropiadas en los principales cambios del	No	La LOTENAL, no celebra sorteos electrónicos.

No.	Objetivo de control	Control	Aplica	Motivo
		sistema, así como, pruebas intrusión para intentar identificar y explotar vulnerabilidades u otras debilidades del sistema.		
		L.6.2.1 Identificación del participante. Debe existir un proceso formal de identificación de participantes.	No	En la página Web de la LOTENAL, no cuenta con venta a través de Internet para los sorteos se hacen a través de un proveedor externo, y en la página Web, sólo se tiene una liga para el juego electrónico.
		L.6.2.2 Cuentas para varios participantes. Debe haber un procedimiento en vigor para el uso de cuentas para varios participantes. En los casos en los que estas no existan, se debe permitir solo una cuenta por participante.	No	En la página Web de la LOTENAL, no cuenta con venta a través de Internet para los sorteos se hacen a través de un proveedor externo, y en la página Web, sólo se tiene una liga para el juego electrónico.
		L.6.2.3 Exclusión de participantes. Debe haber un procedimiento establecido para la	No	En la página Web de la LOTENAL, no cuenta con venta a través de Internet para los sorteos se hacen a través de un proveedor externo, y en la página Web, sólo se tiene una liga para el juego electrónico.

No.	Objetivo de control	Control	Aplica	Motivo
		exclusión de participantes.		
		L.6.2.4 Herramienta para el pago múltiple del participante. Debe haber un procedimiento establecido para asegurar la igualdad de la propiedad entre el titular del tipo de pago y el titular de la cuenta del jugador.	No	En la página Web de la LOTENAL, no cuenta con venta a través de Internet para los sorteos se hacen a través de un proveedor externo, y en la página Web, sólo se tiene una liga para el juego electrónico.
		L.6.3.1 Procedimientos documentados para juegos que se ofrecen en Internet. Las normas establecidas deben incluir el diseño y desarrollo del juego. Además, las reglas del juego deben ser accesibles para los participantes.	No	La LOTENAL no realiza sorteos por Internet.
		L.6.3.2 Aprobación del juego. La versión final del juego debe ser formalmente	No	La LOTENAL no realiza sorteos por Internet.

No.	Objetivo de control	Control	Aplica	Motivo
		aprobada a través de un proceso en el que esté implicada la función de seguridad.		
		L.6.4.1 Recopilación de datos. La recopilación de datos confidenciales, relacionados con el pago, se debe limitar únicamente a los datos estrictamente necesarios para la transacción.	No	La LOTENAL, no celebra sorteos electrónicos; sin embargo el pago de premios tradicional se realiza, con los niveles de seguridad requeridos.
		L.6.4.2 Protección del método de pago. Se tomarán las medidas adecuadas para proteger cualquier tipo de pago, de un uso fraudulento, realizado en el sistema.	No	La LOTENAL, no celebra sorteos electrónicos; sin embargo el pago de premios tradicional se realiza, con los niveles de seguridad requeridos.
		L.6.4.3 Aprobación del servicio de pago. La organización debe verificar que el servicio de pago, garantice la protección de los datos del jugador, incluida cualquier información de identificación personal	No	La LOTENAL, no celebra sorteos electrónicos; sin embargo el pago de premios tradicional se realiza, con los niveles de seguridad requeridos.

No.	Objetivo de control	Control	Aplica	Motivo
		proporcionada por el jugador o los datos relacionados con el pago.		
		L.6.4.4 Registros de la transacción relacionada con los pagos. La organización debe generar todos los registros de las transacciones de cuentas de jugador. Los datos registrados permitirán a la organización rastrear una sola actividad financiera de un jugador de otra transacción.	No	La LOTENAL, no celebra sorteos electrónicos; sin embargo el pago de premios tradicional se realiza, con los niveles de seguridad requeridos.
L7	Apuestas Deportivas.	L.7.1.1 Lista de eventos autorizados. Se debe mantener una lista de los tipos de eventos deportivos autorizados para apuestas.	No	La Entidad no cuenta con juegos deportivos.
		L.7.1.2 Lista de tipos de apuestas autorizadas.	No	La Entidad no cuenta con juegos deportivos.

No.	Objetivo de control	Control	Aplica	Motivo
		Se debe mantener una lista de tipos de apuestas autorizadas para cada deporte ofrecido.		
		L.7.1.3 Lista de opciones de apuestas autorizadas. Se debe mantener una lista de opciones de apuestas por categoría de juego.	No	La Entidad no cuenta con juegos deportivos.
		L.7.1.4 Información sobre la oferta de apuestas. Se deben mantener y publicar: 1) Las condiciones de la oferta de apuestas. 2) Los principios según los cuales se seleccionan los eventos, cómo se fijan y revisan las probabilidades basadas en información publicada, reglas éticas y criterios.	No	La Entidad no cuenta con juegos deportivos.
		L.7.2.1 Selección de eventos.	No	La Entidad no cuenta con juegos deportivos.

No.	Objetivo de control	Control	Aplica	Motivo
		Debe estar en vigor un procedimiento para seleccionar los eventos basándose en la lista de eventos autorizados, a fin de asegurar la integridad de la oferta.		
		L.7.2.2 Fijación y actualización de las probabilidades. Se deben establecer procedimientos para fijar y actualizar las probabilidades y/o bloquear eventos, considerando las fuerzas del mercado. Los procedimientos deben basarse en el respeto a la integridad y el juego responsable y deben asegurar la transparencia.	No	La Entidad no cuenta con juegos deportivos.
		L.7.2.3 Ajuste del nivel de las apuestas al margen. Los niveles autorizados para el margen de cada tipo de apuesta se deben documentar y aprobar.	No	La Entidad no cuenta con juegos deportivos.

No.	Objetivo de control	Control	Aplica	Motivo
		L.7.2.4 Proteger los noveles del pago. La organización debe establecer un conjunto de medidas para garantizar que no se excedan con los niveles de pago autorizados.	No	La Entidad no cuenta con juegos deportivos.
		L.7.3.1 Resultados de eventos finalizados. Debe haber una política, que se base en fuentes confiables, para la confirmación de los resultados. La confirmación de resultados debe hacerse antes de anunciar públicamente los resultados y declarar los ganadores.	No	La Entidad no cuenta con juegos deportivos.
		L.7.3.2 Registros de resultados. Se debe mantener e identificar un registro en respaldo, de todos los resultados como un activo crítico.	No	La Entidad no cuenta con juegos deportivos.
		L.7.4.1	No	La Entidad no cuenta con juegos deportivos.

No.	Objetivo de control	Control	Aplica	Motivo
		Vigilancia de probabilidades. Debe haber un procedimiento para monitorizar todos los cambios de probabilidades y/o bloqueos durante el desarrollo del evento deportivo.		
		L.7.4.2 Vigilancia del mercado. Debe haber un procedimiento para monitorizar el mercado y detectar irregularidades en los eventos o riesgos.	No	La Entidad no cuenta con juegos deportivos.
		L.7.4.3 Vigilancia de las transacciones de los clientes. Debe haber procedimientos ya establecidos para detectar irregularidades en las apuestas. En caso de detección, debe existir un procedimiento establecido que permita notificar a la autoridad	No	La Entidad no cuenta con juegos deportivos.

No.	Objetivo de control	Control	Aplica	Motivo
		reguladora y, si es necesario, al ente deportivo correspondiente.		
		L.7.4.4 Pago en efectivo de las ganancias. Se debe establecer un procedimiento que especifique los umbrales de pago y los métodos de recaudación.	No	La Entidad no cuenta con juegos deportivos.
		L.7.4.5 Seguimiento de los ganadores. De acuerdo a las leyes aplicables, se debe establecer un procedimiento para monitorear a los ganadores sobre una cierta cantidad de ganancias.	No	La Entidad no cuenta con juegos deportivos.
		L.7.4.6 Control de depósitos. Debe establecer un nivel por encima del cual se monitoreen los	No	La Entidad no cuenta con juegos deportivos.

No.	Objetivo de control	Control	Aplica	Motivo
		depósitos de una cierta cantidad.		
		L.7.5.1 Vigilancia de la integridad del evento. Debe haber procedimientos. establecidos para asegurar y documentar la integridad de la oferta de apuesta en vivo.	No	La Entidad no cuenta con juegos en vivo.
		L.7.5.2 Manejo de los resultados en ofertas en vivo. Debe haber procedimientos establecidos para asegurar y documentar la integridad de los resultados durante la oferta de apuesta en vivo. Los aspectos que deben considerarse son el retardo, la fuente para obtener los resultados, la reversión de resultados, entre otros.	No	La Entidad no cuenta con juegos en vivo.
		L.7.5.3	No	La Entidad no cuenta con juegos en vivo.

No.	Objetivo de control	Control	Aplica	Motivo
		Mecanismos de prevención del Courtsiding. Garantizar la protección del cliente y la protección contra el fraude / integridad a través de la provisión de un mecanismo de seguridad, para justificar el retraso en las imágenes en vivo.		
		L.7.6.1 Separación de tareas. Se debe contar con una separación de tareas para asegurar que ningún grupo tenga control total sin supervisión.	No	La Entidad no cuenta con juegos en vivo.
		L.7.6.2 Política corporativa sobre apuestas. Se debe tener una política interna que aborde los derechos de los empleados para jugar.	No	La Entidad no cuenta con juegos en vivo.

No.	Objetivo de control	Control	Aplica	Motivo
L8	Terminales de lotería interactivas en video (VLT).	L.8.1.1 Terminales VLT. Las terminales VLT, deben ser monitoreadas con respecto a la seguridad y porcentaje del pago de premios.	No	La Entidad no cuenta con terminales juego.
		L.8.1.2 Juegos VLT. Las reglas del juego y el porcentaje global de pago de premios estarán disponibles para el cliente.	No	La Entidad no cuenta con terminales juego.
		L.8.1.3 Certificado de juego VLT. Los juegos dedicados para VLT, se probarán y se deberá mantener y emitir un certificado para proporcionar evidencia de integridad.	No	La Entidad no cuenta con terminales juego.
		L.8.1.4 Incidentes VLT. Se debe tener un procedimientos documentados para manejar disputas o protestas del cliente con respecto a una	No	La Entidad no cuenta con terminales juego.

No.	Objetivo de control	Control	Aplica	Motivo
		ganancia o pérdida.		

POLÍTICAS DEL SGSI

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Establecer la realización, seguimiento y aprobación, así como, el cumplimiento de las políticas del SGSI, para la seguridad de la información en la LOTENAL.

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

- **A.5.1 Directrices de gestión de la seguridad de la información.**
  - A.5.1.1 Políticas para la seguridad de la información.
  - A.5.1.2 Revisión de las políticas para la seguridad de la información.

NOMENCLATURA

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

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

POLÍTICAS

PSI - 01	Las políticas para la seguridad de la información deben ser definidas, revisadas y aprobadas por el Grupo Estratégico de la Seguridad de la Información (GESI), mismas que deben ser publicadas y comunicadas a empleados, Organismos de Venta y contratistas externos de la LOTENAL. 5.1.1 **[1]**
PSI – 02	Las políticas de seguridad de la información se deben revisar, actualizar y/o ratificar a intervalos planeados, por el GESI. 5.1.2 **[1]**

POLÍTICAS DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Establecer políticas para la organización de la seguridad de la información con el fin de establecer un marco de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización, estableciendo roles y responsabilidades, segregando tareas y teniendo los contactos con autoridades correspondientes en cuanto a seguridad de la información, así como establecer políticas de seguridad en dispositivos móviles.

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

- **A.6.1 Organización interna**
  - A.6.1.1 Roles y responsabilidades en seguridad de la información,
  - A.6.1.2 Segregación de tareas,
  - A.6.1.3 Contacto con las autoridades,
  - A.6.1.4 Contacto con grupos de interés especial,
  - A.6.1.5 Seguridad de la información en la gestión de proyectos,
- **A.6.2 Los dispositivos móviles y el teletrabajo.**
  - A.6.2.1 Política de dispositivos móviles.

NOMENCLATURA

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

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

POLÍTICAS

POSI-01	El acta de la creación del Comité debe incluir roles y responsabilidades para la administración del mismo, realizando sesiones como mínimo cada dos meses, o la realización de sesiones extraordinarias en caso necesario. A.6.1.1

POSI-02	Deben segregarse las operaciones y responsabilidades de las áreas de la LOTENAL, para evitar que se produzcan modificaciones no autorizadas o usos indebidos de los activos. A.6.1.2
POSI-03	Se debe tener el contacto con otras entidades que proveen servicios como: Públicos, bombero, salud, seguridad, protección civil, proveedores de TI. Para llevar atender incidentes de seguridad de manera rápida y eficaz. A.6.1.3
POSI-04	El Grupo Estratégico de Seguridad de la Información (GESI), debe establecer contacto con organismos especializados en seguridad de la información para mantenerse actualizado y al día en tópicos de Seguridad de la Información, así como, las Gerencias que por su proceso lo necesiten. A.6.1.4.
POSI-05	Independientemente de la naturaleza del proyecto, la seguridad de la información está obligada a tratarse dentro de la gestión de proyectos. A.6.1.5
POSI-06	Todos los empleados que comiencen y/o actualicen algún proyecto deben analizar y ejecutar los controles o requisitos para la seguridad de la información. A.6.1.5
POSI-07	El área responsable debe mantener una administración de las características de los equipos móviles que procesan o almacenan información crítica, así como de los usuarios que los utilizan. A.6.2.1

POSI-08	Todos los dispositivos móviles deben contar con una clave de acceso según las actividades de cada perfil de usuario. A.6.2.1
POSI-09	Las Gerencias que cuenten con dispositivos móviles que salgan fuera de la LOTENAL y que se consideren sustantivos o con un riesgo alto de acuerdo a su información contenida, deben informar a la Gerencia de Centro de Cómputo, para que el equipo sea encriptado o cuente con alguna otra herramienta que resguarde la información. A.6.2.1

POLÍTICAS PARA LA SEGURIDAD RELATIVA A LOS RECURSOS HUMANOS

OBJETIVO

Establecer políticas para asegurarse de que los empleados y contratistas cuenten con las recomendaciones adecuadas corroborar su experiencia y evaluar si son aptos para las funciones para las que se consideran, así mismos asegurar que conozcan y cumplan con sus responsabilidades en seguridad de la información durante y después de la finalización del contrato o cambio en el puesto.

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

- **A.7.1 Antes del empleo**
  - A.7.1.1 Investigación de antecedentes,
  - A.7.1.2 Términos y condiciones del empleo.
- **A.7.2 Durante el empleo**
  - A.7.2.1 Responsabilidades de gestión.
  - A.7.2.2 Concienciación, educación y capacitación en seguridad de la información,
  - A.7.2.3 Proceso disciplinario.
- **A.7.3 Finalización del empleo o cambio en el puesto de trabajo**
  - A.7.3.1 Responsabilidades ante la finalización o cambio.

NOMENCLATURA

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

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

POLÍTICAS

PSRRH-01	La Subgerencia de Empleo debe realizar una verificación de los datos personales, y referencias laborales proporcionados por los candidatos a ocupar una plaza vacante en Lotería Nacional, previo a su contratación. A.7.1.1
PSRRH-02	Cada Gerencia debe realizar una verificación de los datos personales y referencias laborales proporcionados por terceros y/o contratistas con Lotería Nacional, previo a su contratación. A.7.1.1
PSRRH-03	La Subgerencia de Empleo debe establecer claramente los términos y condiciones de contratación de empleados de Lotería Nacional a través de un documento, el cual la Entidad deberá formalizar en conjunto con el candidato.

	A.7.1.2
PSRRH-04	Cada Gerencia debe establecer claramente los términos y condiciones de contratación de terceros y/o contratistas de Lotería Nacional a través de un documento, el cual la Entidad deberá formalizar en conjunto con el candidato. A.7.1.2
PSRRH-05	Cada Gerencia debe difundir y vigilar que el personal, terceras personas y/o contratistas a su cargo cumplan con las políticas de seguridad de la información implementadas en la Lotería Nacional. A.7.2.1
PSRRH-06	Los empleados, personal externo y/o contratistas que se desempeñen dentro de Lotería Nacional deben conocer y acatar los lineamientos de seguridad de la información, además son responsables del uso y mantenimiento de la confidencialidad e integridad de los activos, así como de claves y controles de acceso que les han sido asignados a través de un acuerdo de confidencialidad. A.7.2.1
PSRRH-07	La Subgerencia de Capacitación y Desarrollo debe hacer entrega a todos los empleados de LOTENAL un ejemplar del Código de Ética y Conducta, y los empleados deben firmar la "Carta Compromiso de Conocimiento y Aceptación del Código de Ética y Conducta de Lotería Nacional", así mismo los empleados deben leer, comprender, aplicar los valores contenidos en el mismo. A.7.2.2
PSRRH-08	Todo el personal empleado, contratistas y terceras personas de la Lotería Nacional deben recibir entrenamiento periódico, de seguridad de la información y de competencia de acuerdo a su operación, con el fin de proteger apropiadamente la información, los activos y recursos de la Entidad. A.7.2.2
PSRRH-09	La Subgerencia de Capacitación y Desarrollo debe informar a todos los empleados de nuevo ingreso de LOTENAL, que deben cumplir con el curso de inducción de la Entidad que contiene un panorama general de la entidad (Introducción a la Administración Pública Federal, Misión, Visión, Historia, Sorteos, Normatividad y Prestaciones Institucionales). A.7.2.2
PSRRH-10	La Subgerencia de Empleo debe hacer entrega a los empleados de Lotería Nacional el convenio de confidencialidad, así como las condiciones generales del trabajador, con el fin de que identifiquen sus derechos, obligaciones e incumplimientos. A.7.2.3
PSRRH-11	Al empleado que le hayan hecho u observado alguna violación en la seguridad de la información de la Entidad, debe reportar de manera oficial a la Gerencia de Administración de Personal anexando el acta de

	hechos que se haya levantado por parte del Área, con la evidencia documental o electrónica correspondiente. A.7.2.3
PSRRH-12	La Gerencia de Administración de Personal, debe elaborar los citatorios con 48 horas de anticipación con carácter de estrictamente confidencial para respetar el derecho de audiencia de la persona señalada como presunta responsable de la conducta indebida, señalando el día y hora que se levantara Acta Administrativa. A.7.2.3
PSRRH-13	La Gerencia de Administración de Personal, remitirá a la Dirección Técnica Jurídica el Acta Administrativa con todos sus soportes, para que se dicte opinión técnica jurídica del caso. A.7.2.3
PSRRH-14	La Gerencia de Administración de Personal debe informar el empleado antes de que transcurra un mes desde el día en que se suscitaron los hechos, en caso que proceda aplicar sanción, producto de una amonestación, suspensión de labores sin goce de sueldo o la rescisión laboral. A.7.2.3
PSRRH-15	La Gerencia de Administración de Personal debe archivar en el expediente personal del empleado la opinión técnica jurídica y sus antecedentes, así como el documento que acredita la aplicación de la sanción para que sirva de antecedente en el caso de que el empleado reincida en su conducta para futuras sanciones. A.7.2.3
PSRRH-16	La Gerencia de Administración de Personal genera un aviso de baja con la liberación de responsabilidades del trabajador dirigido a todas las áreas de la Lotería Nacional para la Asistencia Pública, para que las mismas dentro del ámbito de su competencia realicen las acciones que les correspondan. A.7.3.1
PSRRH-17	Todas las Gerencias deben entregar el formato de liberación de responsabilidades a la Gerencia de Administración de Personal una vez que el empleado haya causado baja. A.7.3.1
PSRRH-18	La Gerencias de la Dirección de Informática deben realizar las gestiones necesarias para asegurarse de que el empleado que tiene aviso de baja ya no tiene acceso a los sistemas de la LOTENAL. A.7.3.1
PSRRH-19	Una vez que el empleado de la Lotería Nacional para la Asistencia Pública, haya tenido un cambio de puesto es responsabilidad de la Gerencia de Administración de Personal entregar el nuevo nombramiento. A.7.3.1

POLÍTICAS DE GESTIÓN DE ACTIVOS

OBJETIVO

Establecer políticas para la Identificación de los activos de la organización definiendo las responsabilidades de protección adecuadas junto con ello asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la LOTENAL, así mismo evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información en almacenamiento de medios de información removibles.

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

- **A.8.1 Responsabilidad sobre los activos.**
  - A.8.1.1 Inventario de activos,
  - A.8.1.2 Propiedad de los activos,
  - A.8.1.3 Uso aceptable de los activos,
  - A.8.1.4 Devolución de activos.
- **A.8.2 Clasificación de la información.**
  - A.8.2.1 Clasificación de la información,
  - A.8.2.2 Etiquetado de la información,
  - A.8.2.3 Manipulado de la información.
- **A.8.3 Manipulación de los soportes.**
  - A.8.3.1 Gestión de soportes extraíbles,
  - A.8.3.2 Eliminación de soportes,
  - A.8.3.3 Soportes físicos en tránsito.

NOMENCLATURA

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

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

POLÍTICAS

PGA-01	Las Gerencias al alcance de la certificación deben contar con el inventario de los activos vigentes en el Sistema de Análisis de Riesgos (SAR) y ser identificado claramente su propietario quien debe actualizar el Sistema.

	A.8.1.1 y A.8.1.2
PGA-02	Las Gerencias al alcance de la certificación deben contar con lineamientos específicos para el uso de los activos, mismos que deben darse a conocer a empleados, contratistas y terceros que usan o tienen acceso a los activos de la organización. A.8.1.3
PGA-03	Las Gerencias al alcance de la certificación deben asegurarse que sean devueltos todos los activos de empleados, contratistas y terceros, al término de la relación laboral o contrato, en las condiciones que les fueron entregadas o a satisfacción del propietario del activo, en coordinación con las Gerencias involucradas; así mismo, solicitar que sean cancelados los accesos a sistemas de información y accesos físico y lógico a las instalaciones de la LOTENAL. A.8.1.4
PGA-04	Las Gerencias al alcance de la certificación deben clasificar la información de sus procesos en cumplimiento a lo dispuesto en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental. A.8.2.1
PGA-05	Las Gerencias al alcance de la certificación deben etiquetar la información de acuerdo a lo estipulado en la Ley Federal de Archivos. A.8.2.2
PGA-06	Las Gerencias al alcance de la certificación deben manipular la información con base en el Catálogo de Disposición Documental de la LOTENAL. A.8.2.3
PGA-07	La Gerencia de Centro de Cómputo y Gerencia de Telecomunicaciones deben establecer los mecanismos de control y seguridad sobre el uso, eliminación y soporte de medios de almacenamiento de información removibles. A.8.3.1, A.8.3.2 y A.8.3.3

POLÍTICAS DE CONTROL DE ACCESO

OBJETIVO

Establecer políticas para la administración del Control de Acceso a los Sistemas y servicios de la LOTENAL, así como, el uso adecuado de la contraseña y privilegios.

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

- **A.9.1 Requisitos de negocio para el control de acceso.**
  - A.9.1.1 Política de control de acceso,
  - A.9.1.2 Acceso a las redes y a los servicios de red,
- **A.9.2 Gestión de acceso de usuario.**
  - A.9.2.1 Registro y baja de usuario,
  - A.9.2.2 Provisión de acceso de usuario,
  - A.9.2.3 Gestión de privilegios de acceso,
  - A.9.2.4 Gestión de la Información secreta de autenticación de los usuarios,
  - A.9.2.5 Revisión de los derechos de acceso de usuarios,
  - A.9.2.6 Retirada o reasignación de los derechos de acceso.
- **A.9.3 Responsabilidades del usuario.**
  - A.9.3.1 Uso de la Información secreta de autenticación
- **A.9.4 Controles de acceso a sistemas y aplicaciones.**
  - A.9.4.1 Restricción del acceso a la Información
  - A.9.4.2 Procedimientos seguros de inicio de sesión
  - A.9.4.3 Sistemas de Gestión de contraseñas
  - A.9.4.4 Uso de utilidades con privilegios del Sistema
  - A.9.4.5 Control de acceso al código fuente de los programas

NOMENCLATURA

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

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

POLÍTICAS

PCA-01	Las Gerencias de la Dirección de Informática deben establecer la o las políticas de control de acceso de acuerdo a los servicios que cada una de ellas proporcione. A.9.1.1
PCA-02	La Gerencia de Telecomunicaciones y la Gerencia de Centro de Cómputo deben proporcionar a los usuarios el acceso a la red de acuerdo con los privilegios que les fueron autorizados por el área solicitante. A.9.1.2
PCA-03	Las Gerencias de la Dirección de Informática deben implementar un procedimiento documentado para alta, baja y cambio de usuario de los Sistemas y Servicios de Tecnología de Información (TI). A.9.2.1
PCA-04	Las Gerencias deben solicitar en la forma establecida, el alta, baja y cambio de usuario de los Sistemas y Servicios de TI, de acuerdo a los lineamientos de la Dirección de Informática. A.9.2.2
PCA-05	La Dirección de Informática debe proporcionar el servicio para la asignación de privilegios de los Sistemas y Servicios de TI, así como su administración y control, dependiendo de las funciones y necesidades de las áreas usuarias. A.9.2.3
PCA-06	Toda solicitud de acceso a los Sistemas, Servicios o cambio de privilegios, debe ser autorizado de acuerdo al Manual de Organización de la Lotería Nacional para la Asistencia Pública. A.9.2.3

PCA-07	El acceso a la Infraestructura Tecnológica de la LOTENAL para personal externo debe ser autorizado por personal con nivel mínimo de Gerente del área usuaria y notificar a la Dirección de Informática para su ejecución. A.9.2.3
PCA-08	El Gerente del área usuaria debe notificar al área a la Dirección de Informática el bloqueo temporal del acceso y privilegios a los Sistemas cuando se encuentre de vacaciones un usuario o durante el periodo que no se encuentre laborando por cualquier causa. A.9.2.3
PCA-09	Las Gerencias de la Dirección de Informática deben contar con un proceso para gestionar y administrar la autenticación de los usuarios a los Sistemas y Servicios de la LOTENAL, misma que debe estar protegida y no divulgarse. A.9.2.4
PCA-10	Todas las contraseñas y cuentas de acceso asignadas por default considerando al menos los Sistemas de cómputo de software y Sistemas de base de datos, servidores y dispositivos de red deben cambiarse por el usuario posterior a su instalación y antes de ser utilizados en el ambiente de producción de la LOTENAL. A.9.2.4
PCA-11	Todos los accesos a los sistemas, servicios de TI y privilegios, deben ser revisados por la Dirección de Informática como mínimo una vez al año. A.9.2.5
PCA-12	El acceso a los Sistemas y privilegios concedidos a personal interno y/o externo deben ser deshabilitados en el momento en que termine su relación laboral o contractual, y el área usuaria debe notificar de inmediato al área correspondiente de la Dirección de Informática a través de un oficio, para su cancelación a los Sistemas y privilegios con los que cuente el usuario. A.9.2.6

PCA-13	Cuando un usuario olvida, bloquea o extravía su contraseña, debe solicitar la reactivación o cambio de contraseña de la cuenta del usuario, a través de oficio o correo electrónico a la Dirección de Informática a través del Gerente del área solicitante. A.9.3.1
PCA-14	En ningún caso se debe enviar una contraseña a través de correo electrónico, mensajería instantánea, vía telefónica o cualquier otro medio que no sea de manera presencial; por lo que el usuario debe acudir a recoger la contraseña a la Gerencia de la Dirección de Informática correspondiente. A.9.3.1
PCA-15	Las contraseñas asignadas a un usuario son de uso CONFIDENCIAL, por ende, queda totalmente prohibido su divulgación o préstamo, por lo que será responsable del uso de la misma ante cualquier autoridad interna o externa. El usuario debe memorizar su contraseña de tal manera que no esté escrita en ningún lugar visible que permita su difusión o acceso. A.9.3.1
PCA-16	Las Gerencias de la Dirección de Informática responsables de los aplicativos, deben contar con la segregación de funciones o perfiles de puesto, para restringir el acceso a funciones no autorizadas al usuario. A.9.4.1 y A.9.4.4
PCA-17	Los Sistemas sensibles puestos en producción, así como las bases de datos deben estar aislados y protegidos mediante controles de acceso restringidos. A.9.4.1
PCA-18	Las Gerencias de la Dirección de Informática deben contar con los registros de identificación de usuario a los Sistemas y Servicios, así como la fecha, hora de inicio y terminación de sesión del usuario y administrador del Sistema.

	A.9.4.2 y A.9.4.4
PCA-19	Las Gerencias de la Dirección de Informática deben contar con los registros de intentos fallidos y exitosos de acceso a los Sistemas y Servicios. A.9.4.2
PCA-20	Todas las cuentas de identificación de usuario que no haya registrado actividad alguna en un periodo de sesenta (60) días hábiles, se deben bloquear de manera inmediata. A.9.4.3
PCA-21	Debe existir un mecanismo de control que contenga un historial de contraseñas que prevenga que los usuarios utilicen contraseñas que ya han usado con anterioridad. El historial debe contener por lo menos los últimos cinco (5) contraseñas de cada user-ID. A.9.4.3
PCA-22	Después de tres intentos consecutivos fallidos para introducir la contraseña en el mismo día, el identificador de usuario (user-ID) involucrado debe ser bloqueado, previniendo con esto ataques de adivinación de contraseña. A.9.4.3
PCA-23	La contraseña tendrá una longitud mínima de 8 caracteres alfanuméricos, sensibles a mayúsculas y minúsculas y un tiempo de vida variable dependiendo del Sistema que se utilice asignado por la Gerencia de Centro de Cómputo. A.9.4.3
PCA-24	Las Gerencias de la Dirección de Informática deben contar con un usuario administrador el cual controle, restringa y administre los sistemas y servicios de TI. A.9.4.4

PCA-25	La Gerencia de Centro de Cómputo debe de resguardar el código fuente de todos los Sistemas de la LOTENAL, para evitar el uso inapropiado de actualizaciones innecesarias. A.9.4.5
PCA-26	La actualización del código fuente y bibliotecas del sistema debe ser a través de la Gerencia de Centro de Cómputo. A.9.4.5
PCA-27	La Gerencia de Centro de Cómputo debe mantener un inventario del código fuente y bibliotecas de todos los Sistemas de la LOTENAL. A.9.4.5

POLÍTICAS DE SEGURIDAD PARA EL USO CRIPTOGRÁFICO

OBJETIVO

Garantizar el uso adecuado de la criptografía con el fin de proteger la confidencialidad, autenticidad y/o integridad de la información de los sistemas y bases de datos.

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

- **A.10.1 Controles criptográficos:**
  - A.10.1.1 Política de uso de los controles criptográficos.
  - A.10.1.2 Gestión de claves.

NOMENCLATURA

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

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

POLÍTICAS

PSC-01	Las Gerencias de la Dirección de Informática deben de proteger toda la información considerada como sensible de la LOTENAL con algoritmos de criptográficos seguros desde la solicitud del usuario hasta que llegue la información al mismo. A.10.1.1
PSC-02	Las Gerencias de la Dirección de Informática deben de aplicar algoritmos seguros, para proteger la confidencialidad, autenticidad o integridad de la información de los sistemas o servicios. A.10.1.1
PSC-03	Las Gerencias de la Dirección de Informática deben, revisar el tipo de algoritmo como mínimo una vez por año o cuando la operación lo requiera para definir si se continúa con ese estándar o se debe de cambiar.

	A.10.1.1
PSC-04	Las Gerencias de la Dirección de Informática deben de tomar en cuenta si se encripta la base de datos o la transacción que realiza el sistema, de acuerdo al tipo de protección que requiera la información del sistema. A.10.1.1
PSC-05	Todos los algoritmos criptográficos y medios de encripta miento deben tener un medio de autenticación para usuarios, así como, una vigencia, con el fin de que se puedan administrar y gestionar las claves. A.10.1.2
PSC-06	Las Gerencias de la Dirección de Informática deben de tener un inventario de las claves criptográficas y gestionar su eficacia como mínimo una vez al año. A.10.1.2

POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

OBJETIVO

Establecer políticas para la administración de la SEGURIDAD FÍSICA Y DEL ENTORNO.

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

- **A.11.1 Áreas Seguras.**
  - A.11.1.1 Perímetro de Seguridad Física,
  - A.11.1.2 Controles físicos de entrada,
  - A.11.1.3 Seguridad de oficinas, despachos y recursos,
  - A.11.1.4 Protección contra las amenazas externas y ambientales,
  - A.11.1.5 El trabajo en áreas seguras,
  - A.11.1.6 Áreas de carga y descarga.
- **A.11.2 Seguridad de los equipos**
  - A.11.2.1 Emplazamiento y protección de equipos,
  - A.11.2.2 Instalaciones de suministro,
  - A.11.2.3 Seguridad del cableado,
  - A.11.2.4 Mantenimiento de los equipos,
  - A.11.2.5 Retirada de materiales propiedad de la empresa,
  - A.11.2.6 Seguridad de los equipos fuera de las instalaciones,
  - A.11.2.7 Reutilización o eliminación segura de equipos,
  - A.11.2.8 Equipo de usuario desatendido,
  - A.11.2.9 Política de puesto de trabajo despejado y pantalla limpia.

NOMENCLATURA

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

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

POLÍTICAS

PSFE-01	Los titulares de todas las áreas de la Entidad deben determinar, acreditar y validar si su área debe ser considerada como restringida. A.11.1.1

PSFE-02	Las áreas catalogadas como restringidas, deben implementar y administrar sus respectivas bitácoras para el registro de entrada y salida del personal; quedando como responsables de las actividades que realicen al interior de las mismas. Adicionalmente, se debe implementar algún tipo de control o monitoreo como cámaras, puertas de acceso de personal, cerraduras, dispositivos biométricos, etc. A.11.1.2
PSFE-03	El personal externo debe registrar su entrada y salida del inmueble, dejando una identificación oficial en el módulo de seguridad; el cual, proporciona el gafete de la Entidad que debe portarse de manera visible durante toda la estancia en el inmueble. Si el gafete de la Entidad es extraviado, debe reportarse inmediatamente al módulo de seguridad que autorizó el ingreso y apegarse a lo dispuesto en los procedimientos de la Gerencia de Servicios Generales. No debe permitirse el acceso a ninguna persona sin previa identificación. A.11.1.2
PSFE-04	El personal interno debe portar en todo momento y a la vista, la credencial de la LOTENAL cuando se trata de ingresar al inmueble donde se encuentra su Área de adscripción, así como al ingresar a otros inmuebles de LOTENAL. En el caso, de dirigirse a un Área crítica y/o restringida debe comunicarse directamente con el área responsable para solicitar el acceso físico. Si la credencial de la LOTENAL es extraviada, debe reportarse inmediatamente al Área de personal para su reposición y apegarse a lo dispuesto en los procedimientos de la Gerencia de Servicios Generales. A.11.1.2
PSFE-05	El personal que traiga consigo, equipo de cómputo, de comunicaciones (cámaras de video, fotográficas, equipo de audio y cualquier otro tipo de equipo de grabación), medios de almacenamiento y herramientas, que no sean propiedad de LOTENAL, debe registrarlo en las bitácoras de la Subgerencia de Seguridad y Vigilancia, especificando las características del equipo y cotejar las mismas al salir del inmueble. A.11.1.2
PSFE-06	Todos los portafolios, maletas, bolsas de mano y otro tipo de equipaje deben abrirse y mostrar su contenido a los guardias de seguridad al ingresar y salir de las instalaciones de LOTENAL. A.11.1.2

PSFE-07	Queda prohibida la introducción de cualquier tipo de arma (navajas, pistolas, rifles, etc.), sustancias inflamables y explosivas, así como material que pueden poner en riesgo la integridad física de las personas y de los bienes de la LOTENAL que se encuentren en las instalaciones de la LOTENAL, salvo que se cuente con la autorización correspondiente. A.11.1.2
PSFE-08	Los empleados son responsables de resguardar en su área de trabajo (oficinas y cubículos) la documentación, materiales y objetos personales que se encuentren en ellos. Las oficinas, gavetas y escritorios deben cerrarse con llave en caso de ausencia del personal. A.11.1.2
PSFE-09	El directorio telefónico interno debe contener solamente el nombre y extensión del personal del área inscrito en él, en caso de que éste se encuentre a la vista. A.11.1.3
PSFE-10	La Gerencia de Servicios Generales debe colocar detectores de humo y extintores en todas las áreas, que permitan mitigar el riesgo de un incendio. Estos dispositivos deben contar con el mantenimiento adecuado. A.11.1.3
PSFE-11	La Gerencia de Servicios Generales debe colocar letreros que indiquen al personal las rutas de evacuación de las instalaciones de LOTENAL en cualquier lugar donde se encuentren, así como también las indicaciones de ¿qué hacer? conforme lo indica la regulación existente para tal efecto. A.11.1.3
PSFE-12	Se debe contar con los planos de construcciones, originales y actualizados de las instalaciones, para ser utilizados en caso de contingencia. A.11.1.3
PSFE-13	La Gerencia de Servicios Generales, en apego a la infraestructura física de sus inmuebles debe cumplir con las disposiciones oficiales que en materia de protección civil se requiere. Asimismo, la Gerencia debe contar con un programa que incluya revisiones periódicas del equipo e infraestructura contra incendio. A.11.1.4

PSFE-14	En caso de ocurrir un siniestro o contingencia, las instalaciones alternas utilizadas deben contar con los equipos de reemplazo y/o respaldo adecuados. A.11.1.4
PSFE-15	La Gerencia de Servicios Generales debe contar con un equipo de Brigadistas que cuente con los elementos suficientes para enfrentar situaciones de siniestros, temblores o amenazas externas, con la finalidad de salvaguardar los recursos humanos y materiales. Los brigadistas deben recibir capacitación mínima una vez al año, con el fin de poder enfrentar situaciones de siniestros, temblores o amenazas externas y así salvaguardar los recursos humanos y materiales. A.11.1.4
PSFE-16	Todo el personal de las Gerencias es responsable de mantener sus espacios limpios y libres de objetos que puedan entorpecer las rutas de evacuación establecidas, asimismo, la Gerencia de Servicios Generales a través de sus áreas adscritas, debe conservar despejado los espacios cuando se trate de labores de mantenimiento y obras públicas en caso de una contingencia. A.11.1.5
PSFE-17	Las áreas que tengan identificadas zonas de carga y descarga de insumos, son responsables de implementar los controles que consideren adecuados para restringir el acceso físico a las mismas o hacia otras áreas administrativas, asimismo, deben informar a la Gerencia de Servicios Generales cuando requieran ingresar materiales, herramientas, instrumentos, entre otros, para su validación en las zonas. A.11.1.6
PSFE-18	El material que ingresa al área de carga y descarga debe ser revisado por personal autorizado de la LOTENAL, para evitar la introducción de posibles amenazas. A.11.1.6
PSFE-19	Las áreas administrativas deben coordinar con la Gerencia de Servicios Generales, la colocación de equipos, servidores, redes, entre otros, para garantizar que no incurran en riesgos y/o vulnerabilidades. A.11.2.1
PSFE-20	Los empleados no tienen autorización para reasignar o prestar el equipo de cómputo que tienen a su resguardo para el desempeño de sus labores.

	a menos qué se cuente con la autorización por escrito del Gerente del área correspondiente. A.11.2.1
PSFE-21	La Gerencia de Servicios Generales, a solicitud de las áreas administrativas, apoyará con el mantenimiento preventivo y/o correctivo de la infraestructura física de las instalaciones eléctricas, equipos, cableado eléctrico, servidores y comunicaciones de TI, con el fin de evitar interrupciones en los procesos de la LOTENAL. A.11.2.2
PSFE-22	Los equipos de cómputo y dispositivos de seguridad deben tener el mantenimiento preventivo y/o correctivo adecuado, según se establezca en los respectivos programas de trabajo, a través de la Gerencia de Centro de Cómputo, Gerencia de Telecomunicaciones o la Gerencia de Servicios Generales, según sea el caso así mismo se debe proteger por medios físicos adecuados todo cableado eléctrico y de comunicaciones para evitar la desconexión accidental o dolosa. A.11.2.3
PSFE-23	Durante la relación laboral, el personal con resguardo de activos de TI, es responsable de tramitar la autorización de salida correspondiente y dar aviso al área de seguridad para validar la misma en el punto de acceso. Al término de la relación contractual, el personal debe hacer entrega de sus activos a su área de adscripción, quien, a su vez, informará al área de seguridad para vigilar y controlar los puntos de acceso. A.11.2.5
PSFE-24	Las Gerencias de Centro de Cómputo deben establecer medidas de seguridad a los equipos que salgan fuera de las instalaciones de la LOTENAL como la encriptación, tomando en cuenta los diferentes riesgos que conlleva trabajar fuera de dichas instalaciones. A.11.2.6
PSFE-25	La Gerencia de Centro de Cómputo debe contar con las herramientas necesarias para verificar el correcto eliminado de todos los registros de los soportes de almacenamiento de manera segura, antes de deshacerse de ellos o de su reutilización. A.11.2.7
PSFE-26	La Gerencia de Centro de Cómputo debe contar con las herramientas necesarias para bloquear los equipos que estén inactivos.

	A.11.2.8
PSFE-27	Los empleados y proveedores que tengan equipos de cómputo son responsables de bloquear el equipo al levantarse de su lugar de trabajo. A.11.2.9

POLÍTICAS DE SEGURIDAD DE LAS OPERACIONES

OBJETIVO

Establecer políticas para la administración de Seguridad de las operaciones.

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

- **A.12.1 Procedimientos y responsabilidades operacionales**
  - A.12.1.1 Documentación de procedimientos de las operaciones
  - A.12.1.2 Gestión de cambios
  - A.12.1.3 Gestión de capacidades
  - A.12.1.4 Separación de los recursos de desarrollo, prueba y operación
- **A. 12.2 Protección contra el software malicioso (Malware)**
  - A.12.2.1 Controles contra el código malicioso
- **A.12.3 Copias de seguridad**
  - A.12.3.1 Copias de seguridad de la información
- **A.12.4 Registros y supervisión**
  - A.12.4.1 Registro de eventos
  - A.12.4.2 Protección de la información de registro
  - A.12.4.3 Registros de administración y operación
  - A.12.4.4 Sincronización del reloj
- **A.12.5 Control del software en explotación**
  - A.12.5.1 Instalación del software en explotación
- **A.12.6 Gestión de la vulnerabilidad técnica**
  - A.12.6.1 Gestión de las vulnerabilidades técnicas
  - A.12.6.2 Restricción en la instalación del software
- **A.12.7 Consideraciones sobre la auditoria de sistemas de información**
  - A.12.7.1 Controles de auditoria de sistemas de información

NOMENCLATURA

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

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

POLÍTICAS

PSO-01	Deben documentarse y mantenerse disponibles los procedimientos de operación y del SGSI, así como, ser difundidos en el SIGEC, para todos los usuarios de la LOTENAL A.12.1.1
PSO-02	La Gerencia de Sistemas Sustantivos, debe documentar y registrar cualquier cambio en los sistemas, así como, las actualizaciones implementadas y pruebas necesarias para verificar dichos cambios que no afecten el buen funcionamiento de los demás Sistemas de la LOTENAL. A.12.1.2
PSO-03	La Gerencia de Centro de Cómputo debe asegurar el buen desempeño de los Sistemas mediante monitoreo, adecuación y proyección del uso de los recursos de la LOTENAL. A.12.1.3
PSO-04	La Gerencia de Centro de Cómputo debe mantener íntegros, disponibles y confiables los registros en los ambientes de desarrollo, prueba y producción y definir en conjunto con la Gerencia de Sistemas Sustantivos los roles, responsabilidades y claves de accesos a los sistemas. A.12.1.4
PSO-05	La Gerencia de Centro de Cómputo debe implementar controles de detección, prevención y recuperación en todos los equipos de Cómputo, que sirvan para mitigar el riesgo de las vulnerabilidades, contra software y código malicioso que afecte el sistema operativo y los programas del equipo, así como la información y funcionamiento del antivirus. A.12.2.1
PSO-06	La Gerencia de Centro de Cómputo debe hacer respaldos periódicos de la información sensible contenida en los servidores de la LOTENAL, así como de los aplicativos. A.12.3.1

PSO-07	La Gerencia de Centro de Cómputo debe registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información en los servidores y sistemas. A.12.4.1
PSO-08	La Gerencia de Centro de Cómputo debe administrar y proteger los registros de los LOGS para identificar cualquier tipo de acceso mal intencionado que pudiera manipular la Información. A.12.4.2
PSO-09	La Gerencia de Centro de Cómputo debe contar con los registros de actividades que realice el administrador y los operadores del Sistema, para mantener la integridad en la operación. A. 12.4.3
PSO-10	La Gerencia de Centro de Cómputo debe configurar el protocolo de tiempo de red NTP, en todos los servidores de la Entidad, para que se sincronicen con el controlador de dominio principal (Directorio Activo). A.12.4.4
PSO-11	La Gerencia de Centro de Cómputo es la única autorizada para instalar o desinstalar cualquier tipo de software en los equipos, por lo que deberá establecer un mecanismo de control para evitar que los usuarios instalen software de cualquier tipo sin su autorización, asimismo deberá realizar auditorías continuas al software instalado en los equipos propiedad de la LOTENAL. A.12.5.1 y 12.6.2
PSO-12	La Gerencia de Centro de Cómputo debe obtener información oportuna acerca de las vulnerabilidades en los sistemas operativos y aplicativos para mitigar los riesgos en los sistemas A.12.6.1
PSO-13	La Gerencia de Centro de Cómputo deberá planear y programar las actividades de auditoría a los Sistemas Operativos y Aplicativos, para minimizar el riesgo de interrupciones en los procesos del negocio. A.12.7.1

PSO-14	La Gerencia de Centro de Cómputo debe administrar el acceso a los sistemas para una auditoría previa solicitud de las unidades administrativas de LOTENAL y dicho acceso debe de ser de sólo lectura. A.12.7.1

POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

OBJETIVO

Establecer políticas para la administración de la seguridad de las comunicaciones.

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

- **A.13.1 Gestión de la seguridad de redes**
  - A.13.1.1 Controles de red.
  - A.13.1.2 Seguridad de los servicios de red.
  - A.13.1.3 Segregación en redes.
- **A.13.2 Intercambio de información**
  - A.13.2.1 Políticas y procedimientos de intercambio de información.
  - A.13.2.2 Acuerdos de intercambio de información.
  - A.13.2.3 Mensajería electrónica.
  - A.13.2.4 Acuerdos de confidencialidad o no revelación.

NOMENCLATURA

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

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

POLÍTICAS

PSCOM-01	La Gerencia da Telecomunicaciones es la responsable da administrar los dispositivos y servicios que permitan mantener la Seguridad Informática dentro da la red de la LOTENAL. A.13.1.1
PSCOM -02	La Gerencia de Telecomunicaciones debe contar con una infraestructura de información donde se lleve a cabo la separación de Sistemas de Información sensibles con la red de usuarios internos, controlando y monitoreando la interacción de una red con la otra de la LOTENAL. A.13.1.1

PSCOM-03	La Gerencia de Telecomunicaciones es la responsable de administrar los dispositivos y servicios que permitan mantener la Seguridad Informática dentro de la red de LOTENAL. A.13.1.2
PSCOM-04	La Gerencia de Telecomunicaciones debe verificar que el proveedor de servicios de Red, cumpla con las especificaciones del anexo técnico y éstos se encuentren estipulados en cada uno de los contratos de mantenimiento a la Infraestructura de Comunicaciones y Sistemas de Seguridad Informática. A.13.1.2
PSCOM-05	La Gerencia de Telecomunicaciones es la encargada de que los servicios de Información, los usuarios y Sistemas de Información estén separados en distintas redes. A.13.1.3
PSCOM-06	La Gerencia al alcance de la certificación debe establecer los mecanismos de control para el cumplimiento de las políticas y procedimientos que protejan el intercambio de información mediante el uso de todo tipo de recursos de la Comunicación en la LOTENAL. A.13.2.1
PSCOM-07	Todas las unidades administrativas de la LOTENAL que realicen algún intercambio de información con un tercero, deberán establecer un convenio de confidencialidad en el que incluya las permisiones y prohibiciones (los roles, niveles de acceso y restricciones acerca del uso de los activos de información) sobre la manipulación y divulgación de información del negocio y software entre ambas partes y realizar las modificaciones y actualizaciones a que haya lugar, cuando se requiera. A.13.2.2, A.13.2.4
PSCOM-08	La Gerencia de Centro de Cómputo debe administrar las cuentas de correo electrónico, asignando privilegios a los usuarios dependiendo de su perfil laboral y estos se mantendrán monitoreados; en caso de que se solicite la suspensión de la cuenta, debe ser deshabilitada por el periodo solicitado, de acuerdo a la normatividad vigente, más no eliminada. A.13.2.3

PSCOM-09	Los servicios de mensajería instantánea estarán restringidos, salvo cuando exista la justificación y autorización por parte del Director de Área solicitante, mediante el formato F38.40, debidamente requisitado y establecido para tal fin. A.13.2.3
PSCOM-10	Los privilegios para claves telefónicas, acceso a Internet y correo electrónico no deben ser utilizados para fines ajenos al desempeño de las funciones de los trabajos encomendados por la LOTENAL y la utilización de los mismos estará supeditada a contar con la justificación y autorización por parte del Director de Área solicitante, para el caso de las claves telefónicas y acceso a Internet; y por el Gerente para el caso del correo electrónico, mediante el formato establecido para tal fin. A.13.2.3

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

OBJETIVO

Establecer políticas para la administración de adquisición, desarrollo y mantenimiento de los sistemas de información.

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

- **A.14.1 Requisitos de seguridad en sistemas de información**
  - A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información.
  - A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas.
  - A.14.1.3 Protección de las transacciones de servicios de aplicaciones.
- **A.14.2 Seguridad en el desarrollo y en los procesos de soporte**
  - A.14.2.1 Política de desarrollo seguro.
  - A.14.2.2 Procedimiento de control de cambios en sistemas
  - A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - A.14.2.4 Restricciones a los cambios en los paquetes de software.
  - A.14.2.5 Principios de ingeniería de sistemas seguros.
  - A.14.2.6 Entorno de desarrollo seguro.
  - A.14.2.7 Externalización del desarrollo de software.
  - A.14.2.8 Pruebas funcionales de seguridad de sistemas.
  - A.14.2.9 Pruebas de aceptación de sistemas.
- **A.14.3 Datos de prueba**
  - A.14.3.1 Protección de los datos de prueba.

NOMENCLATURA

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

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

POLÍTICAS

PADMSI-01	Las Gerencias de la Dirección de Informática deben analizar y determinar el tipo y nivel de seguridad para los nuevos desarrollos del software o para los sistemas que se adquieren por un proveedor, así como para sus actualizaciones. A.14.1.1
PADMSI-02	Las Gerencias de la Dirección de Informática deben proteger la información de las aplicaciones que manejan información sensible. A.14.1.2
PADMSI-03	Las Gerencias de la Dirección de Informática deben determinar el tipo y nivel de seguridad adecuada para los registros que viajan a través de redes públicas con el fin de proteger la información. A.14.1.2
PADMSI-04	Las Gerencias de la Dirección de Informática deben contar con los mecanismos y herramientas de Desarrollo de Sistemas para asegurar la integridad y seguridad de la información. A.14.1.3
PADMSI-05	La Gerencia de Sistemas Sustantivos debe contar con la documentación formal de los requerimientos específicos del cliente o el área solicitante para comenzar con un desarrollo o mantenimiento del sistema. A.14.2.1
PADMSI-06	La Gerencia de Sistemas Sustantivos debe realizar un análisis con el área solicitante para identificar el tipo y nivel de seguridad que debe tener el desarrollo o mantenimiento del sistema, con el fin de cumplir con los niveles de confidencialidad. A.14.2.1
PADMSI-07	Los sistemas que desarrolle la Gerencia de Sistemas Sustantivos deben contar un módulo de administración de usuarios, que permita la creación de perfiles y privilegios con el fin de salvaguardar la información. A.14.2.1

PADMSI-08	La Gerencia de Sistemas Sustantivos debe Gestionar con las otras Gerencias de la Dirección de Informática los recursos necesarios tales como infraestructura de cómputo, comunicaciones y licenciamiento para el desarrollo o mantenimiento del sistema. A.14.2.1
PADMSI-09	La Gerencia de Centro de Cómputo debe proveer a la Gerencia de Sistemas Sustantivos los ambientes de desarrollo, prueba y producción, para los desarrollos y/o mantenimientos que se realicen en la LOTENAL. A.14.2.1
PADMSI-10	La Gerencia de Centro de Cómputo debe contar con un registro formal de control de cambios para las versiones y la configuración del sistema durante el ciclo de vida del mismo. A.14.2.2
PADMSI-11	La Gerencia de Sistemas Sustantivos en conjunto con las áreas responsables de los cambios efectuados a las aplicaciones, deben realizar las pruebas necesarias previas a la liberación de la aplicación, con el fin de verificar que no existen efectos adversos en las operaciones. A.14.2.3
PADMSI-12	La Gerencia de Sistemas Sustantivos debe realizar un análisis profundo para la actualización o modificación de los sistemas tomando en cuenta la licencia correspondiente del sistema en caso de que aplique. A.14.2.4
PADMSI-13	La Gerencia de Sistemas Sustantivos debe contar con la documentación formal para el diseño, la programación, la implantación y el mantenimiento de los sistemas que desarrolle en la LOTENAL. A.14.2.5
PADMSI-14	Las Gerencias de la Dirección de Informática deben proporcionar los recursos necesarios para el desarrollo de los sistemas, como la infraestructura, personal, comunicación de voz y datos durante el ciclo de vida del desarrollo del sistema. A.14.2.6
PADMSI-15	Cuando se contrate un desarrollo o mantenimiento de sistemas, las Gerencias de la Dirección de Informática deben asegurarse que se cumplan con las

	especificaciones técnicas solicitadas a través de una entrega formal por parte del proveedor. A.14.2.7
PADMSI-16	La Gerencia de Sistemas Sustantivos debe permitir los accesos necesarios a todo el personal que participe en el desarrollo o mantenimiento del sistema con el fin de que se ejecuten pruebas unitarias al sistema. A.14.2.8
PADMSI-17	La Gerencia de Sistemas Sustantivos debe realizar pruebas en el ambiente de desarrollo, en el ambiente de pruebas y QA con el usuario final del sistema para los desarrollos o mantenimiento para la liberación del sistema a producción. A.14.2.9
PADMSI-18	La Gerencia de Sistemas Sustantivos debe contar con la documentación formal de la liberación del desarrollo o mantenimiento de sistemas. A.14.2.9
PADMSI-19	La Gerencia de Sistemas Sustantivos debe de realizar los manuales de usuario y técnicos de los sistemas desarrollados para la LOTENAL. A.14.2.9
PADMSI-20	Para la liberación del sistema en ambiente productivo la Gerencia de Sistemas Sustantivos debe contar con la documentación formal de aceptación final del Gerente o funcionario solicitante, con el fin de verificar el cumplimiento de los servicios o productos determinados en la solicitud. A.14.2.9
PADMSI-21	Una vez aceptado el sistema, debe migrarse a un ambiente de producción y la Gerencia de Centro de Cómputo es la única facultada para la liberación en ambiente productivo. A.14.2.9
PADMSI-22	Se debe dar protección a los datos utilizados en las pruebas de software, así como no correr las aplicaciones finales en un ambiente de pruebas o preproducción fuera de las instalaciones designadas por la LOTENAL. A.14.3.1

POLÍTICAS DE RELACIÓN CON PROVEEDORES

OBJETIVO

Establecer políticas para la administración de relación con proveedores para proteger los Activos del SGSI.

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

- **A.15.1 Seguridad en las relaciones con proveedores**
  - A.15.1.1 Política de seguridad de la información en las relaciones con los proveedores.
  - A.15.1.2 Requisitos de seguridad en contratos con terceros.
  - A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones.
- **A.15.2 Gestión de la provisión de servicios del proveedor.**
  - A.15.2.1 Control y revisión de la provisión de servicios del proveedor.
  - A.15.2.2 Gestión de cambios en la provisión del servicio del proveedor.

NOMENCLATURA

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

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

POLÍTICAS

PRP-01	Cada Gerencia que por su operación tenga alguna relación con proveedores, contratistas o terceros debe establecer claramente los términos y condiciones del servicio, a través de un documento de contratación formalizado con el proveedor, contratista o terceros. A.15.1.1
PRP-02	Cada Gerencia que por su operación tenga alguna relación con proveedores, contratistas o terceros debe acordar por medio contractual a que va a tener acceso ya sea físico, documental y/o lógico, con el fin de prevenir fuga o mala manipulación de la información. A.15.1.2

PRP-03	Cada Gerencia que por su operación tenga alguna relación con proveedores, contratistas o terceras personas debe verificar con el Área Jurídica para que se incluya en el contrato el convenio de confidencialidad con el fin de proteger los activos de información de la LOTENAL. A.15.1.2
PRP-04	Las Gerencias de la Dirección de Informática deben de contar con los lineamientos contractuales con los proveedores de Tecnología de la Información (TI) de los servicios y/o de los productos que van a ser realizados o entregados para la operación de la Entidad. A.15.1.3
PRP-05	Cada Gerencia que por su operación tenga alguna relación con proveedores, contratistas o terceros debe supervisar y monitorear que los servicios y/o productos entregados cumplan en tiempo y forma con lo establecido en el contrato, con el fin de tener un nivel de servicio adecuado en la LOTENAL. A.15.2.1
PRP-06	Cada Gerencia que por su operación tenga alguna relación con proveedores, contratistas o terceros debe tomar en cuenta los cambios o actualizaciones del servicio y/o productos que se tengan que hacer con proveedores, contratistas o terceros con el fin de no poner en riesgo lo operación de la LOTENAL. A.15.2.2

POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Establecer políticas para la Gestión de Incidentes de Seguridad de la Información.

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

- **A.16.1 Gestión de incidentes de seguridad de la información y mejoras**
  - A.16.1.1 Responsabilidades y procedimientos.
  - A.16.1.2 Notificación de los eventos de seguridad de la información.
  - A.16.1.3 Notificación de puntos débiles de la seguridad
  - A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
  - A.16.1.5 Respuesta a incidentes de seguridad de la información
  - A.16.1.6 Aprendizaje de los incidentes de seguridad de la información
  - A.16.1.7 Recopilación de evidencias

NOMENCLATURA

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

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

POLÍTICAS

PGISI-01	Las Gerencias de la Dirección de Informática deben contar con los mecanismos apropiados para la atención y seguimiento de los incidentes de seguridad de hardware y software para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información que se lleguen a presentar. A.16.1.1
PGISI-02	La Gerencia de Servicios Generales debe contar con los mecanismos apropiados para la atención y seguimiento de los incidentes de seguridad física e inmuebles para garantizar una respuesta rápida, efectiva y adecuada a los incidentes que se lleguen a presentar. A.16.1.1