



PLAN DE SEGURIDAD, PRIVACIDAD Y TRATAMIENTO DE RIESGOS DE LA INFORMACIÓN – EMSA

POLITICAS DE SISTEMAS EMSA

Propósito:

- Asegurar la integridad, confidencialidad de la información y los recursos relacionados.
- Investigar posibles incidentes de seguridad para garantizar el cumplimiento de las políticas de seguridad de la empresa.
- Monitorear las actividades relacionadas con los sistemas de usuarios cuando se considere apropiado

ALCANCE DE LAS POLÍTICAS

Describir las políticas de sistemas, anuncia los principales lineamientos en relación con aspectos generales de la informática con sistemas de información que apoyan la gestión administrativa, equipos de cómputo y seguridad informática.

Esta política aplica a todos funcionarios que utilizan tecnologías de información y de comunicaciones y aplica a los equipos y software propios de la entidad

RESPONSABLE

El profesional de sistemas será el responsable del mantenimiento y revisión periódica de este documento de tal forma que tenga en cuenta cambios tecnológicos y los cambios que ocurra en la organización o nuevas normas jurídicas que afecten las políticas aquí enunciadas.

POLITICA DE INFORMATICA Y COMUNICACIONES

- Mejorar el efecto de la función de los sistemas y los recursos informáticos en las actividades propias de la empresa. Es compromiso de cada funcionario usuario de un computador, de los servicios y de las redes, conocer estas políticas y acatarlas durante el desarrollo de sus funciones.
- Debe existir la cultura informática en la empresa, para lograr que los usuarios tomen conciencia de que los documentos críticos desde el punto de vista del negocio, deben residir en un directorio de su PC en Mis documentos\EMSA ## (## Numero que tiene asignado el usuario).



LOTERÍA DE MANIZALES

PARA GANARLA HAY QUE COMPRARLA

- Todos los funcionarios de EMSA deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades.
- Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la Entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la Entidad.
- Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la Entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.
- Todas las prerrogativas para el uso de los sistemas de información de la Entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la Entidad.

POLITICA DE ADMINISTRACION DE CAMBIOS

- Los cambios en la plataforma tecnológica deben quedar documentados desde su solicitud hasta su implantación, lo que proveerá de herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.
- Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.
- Los servicios informáticos se brindaran en función de los recursos disponibles y las prioridades establecidas por la directiva Gerencial.
- El profesional sistemas definirá un esquema para la recepción y atención de las solicitudes de servicios que tengan que ver con recursos informáticos y de comunicaciones.
- EMSA velara través de sistemas por el buen funcionamiento de los recursos informáticos.

POLITICA DE SEGURIDAD DE LA INFORMACION

- Los funcionarios públicos y el proveedor de software son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la Entidad, por la Ley para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.
- Los funcionarios EMSA y el proveedor, no deben suministrar información de la entidad a ningún ente externo sin las autorizaciones respectiva de la Gerencia.

 Calle 51C Carrera 15B Barrio La Asunción.
Manizales, Colombia

 PBX: (606) 8841927

 www.loteriademanizales.com

 Línea de Atención al Cliente 018000423806

 emsa.loteriademanizales@gmail.com
loteriademanizales@une.net.co
notificacionesjudiciales@loteriademanizales.com



LOTERÍA DE MANIZALES

PARA GANARLA HAY QUE COMPRARLA

- Todo funcionario que utilice los recursos Informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje.
- Los funcionarios y el proveedor cuando dejen de prestar sus servicios a la Entidad, se compromete entregar toda la información respectiva de su trabajo realizado. Una vez retirado el funcionario y/o proveedor, deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo, los funcionarios públicos que detecten el mal uso de la información esta en la obligación de reportar el hecho a la Oficina Jurídica de la entidad.
- El profesional de sistemas no violará el derecho a la privacidad y confidencialidad de los datos colocados en los sistemas de información en general en la empresa, solo se permitirá el acceso a la información propia de los usuarios cuando se solicitado de manera formal por una un funcionario competente con la respectiva justificación.
- Sistemas velara por que se establezcan sistemas de protección, sistemas de detección de ataques informáticos y la creación de procedimientos de recuperación de los sistemas en caso de ocurrencia de incidentes.

POLITICA DE SEGURIDAD PARA LOS SERVICIOS INFORMATICOS

- El sistema de correo electrónico y grupos de charla de la entidad deben ser usados únicamente para el ejercicio de las funciones de competencia de cada funcionario.
- Los funcionarios EMSA y/o proveedores que hayan recibido aprobación para tener acceso a Internet a través de las facilidades de la entidad, deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.
- Si los usuarios sospechan que hay infección por un virus, deben inmediatamente informar al profesional de sistemas y no utilizar el computador.

POLITICA DE SEGURIDAD EN RECURSOS INFORMATICOS

- Administración de usuarios: Establecer como deben ser utilizadas las claves de ingreso a los recursos informáticos. Dar los parámetros sobre la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas.
- Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, definiendo las acciones permitidas por cada uno de estos. Deberán permitir la asignación a cada usuario de posibles y diferentes roles.

 Calle 51C Carrera 15B Barrio La Asunción.
Manizales, Colombia

 PBX: (606) 8841927

 www.loteriademanizales.com

 Línea de Atención al Cliente 018000423806

 emsa.loteriademanizales@gmail.com
loteriademanizales@une.net.co
notificacionesjudiciales@loteriademanizales.com



LOTERÍA DE MANIZALES

PARA GANARLA HAY QUE COMPRARLA

- El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.
- Las palabras claves o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.
- Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
- Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.
- Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.
- El profesional de sistemas definirá el esquema para garantizar el mantenimiento de los PCs e impresoras.
- La infraestructura tecnológica que soporta los servicios telemáticos y los sistemas de información de apoyo a la gestión administrativa será administrada por el profesional de sistemas.

POLITICA DE SEGURIDAD EN COMUNICACIONES

- Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratados como información confidencial.
- Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la entidad, debe pasar a través de los sistemas de defensa electrónica que incluyen servicios de ciframiento y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.
- Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá estar cifrada

POLITICA DE SOFTWARE UTILIZADO

- Todo software que utilice EMSA será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la Entidad o reglamentos internos.

 Calle 51C Carrera 15B Barrio La Asunción.
Manizales, Colombia

 PBX: (606) 8841927

 www.loteriademanizales.com

 Línea de Atención al Cliente 018000423806

 emsa.loteriademanizales@gmail.com
loteriademanizales@une.net.co
notificacionesjudiciales@loteriademanizales.com



LOTERÍA DE MANIZALES

PARA GANARLA HAY QUE COMPRARLA

- Debe existir una cultura informática al interior de la Entidad que garantice el conocimiento por parte de los funcionarios, de las implicaciones que tiene el instalar software ilegal en los computadores de EMSA.
- Existirá un inventario de las licencias de software de EMSA que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.
- Los sistemas de información de apoyo a gestión administrativa están regidos por los derechos de autor que se lleve acabo entre las partes.

POLITICA DE ACTUALIZACION DE HARDWARE

- Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del Profesional de sistemas.
- La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.
- Los equipos (PC, servidores, LAN etc.) no deben moverse o reubicarse sin la aprobación previa del profesional de sistemas.
- EMSA debe tener un proveedor del servicio de Internet para toda la entidad.
- El esquema de las redes LAN será definido por EMSA.

POLITICA DE ALMACENAMIENTO Y RESPALDO

- La información que es soportada por la infraestructura de sistemas deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.
- Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.
- La entidad definirá la custodia de los respaldos de la información que se realizará externamente.
- El almacenamiento de la información deberá realizarse interna y/o externamente a la Entidad, de acuerdo con la importancia de la información.
- El área dueña de la información en conjunto con la oficina Sistemas definirán la estrategia a seguir para el respaldo de la información.
- Los funcionarios de EMSA son responsables de los respaldos de su información en los PCs, siguiendo las indicaciones técnicas dictadas por la oficina de Sistemas. La oficina de Sistemas será la autorizada para realizar el seguimiento y control de esta política.

 Calle 51C Carrera 15B Barrio La Asunción.
Manizales, Colombia

 PBX: (606) 8841927

 www.loteriademanizales.com

 Línea de Atención al Cliente 018000423806

 emsa.loteriademanizales@gmail.com
loteriademanizales@une.net.co
notificacionesjudiciales@loteriademanizales.com



POLITICA DE CONTINGENCIA

- La Entidad debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, incendio, explosión, terrorismo, inundación etc.

POLITCA DE AUDITORIA

- Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la Entidad, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones debengenerar pistas (adición, modificación, borrado) de auditoria.
- Todos los archivos de auditorias deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.
- Todos los archivos de auditorias de los diferentes aplicativos deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.
- Todos los archivos de auditorias deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas.
- Todos los computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.
- La interventoría de los contratos de soporte y mantenimiento de los sistemas de apoyo será asumida por el profesional de sistemas.

POLITICA DE SEGURIDAD FISICA

- La Entidad deberá contar con los mecanismos de control de acceso como: puertas de seguridad, sistema de alarmas y circuitos cerrados de televisión en las dependencias que la entidad considere críticas.
- El área de Sistemas es de acceso restringido y cualquier persona que ingrese a ella deberá estar acompañada permanentemente por el personal que labora cotidianamente en este lugar.
- Toda persona que se encuentre dentro de la entidad deberá portar su identificación en lugar visible, en el área de Sistemas y las que la entidad considere criticas deberá existir elementos de control de incendio, inundación y alarmas.



LOTERÍA DE MANIZALES

PARA GANARLA HAY QUE COMPRARLA

- A todos los PCs, módems y equipos de comunicación se deben registrar: su ingreso, salida y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la oficina de Sistemas.
- Los equipos de cómputo (PCs, servidores, equipos de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa de Sistemas.
- Los funcionarios públicos se comprometen a **NO** utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que genere caídas de la energía.
- Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no están autorizados para utilizar los recursos informáticos de la entidad.

POLITICA DE ADMINISTRACION DE LA SEGURIDAD

- La evaluación de riesgos de seguridad para los recursos Informáticos en producción se debe ejecutar al menos una vez al año. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.
- Cualquier sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecte, en forma inmediata al área de Sistemas.

REGISTROS

1. Registros De accesos realizados por Usuarios
2. Registros de recepción y atención a solicitudes de usuarios

El presente Plan de Seguridad, Privacidad y Tratamiento de Riesgos de la Información – EMSA, tiene articulación con los contenidos y alcances contemplados en los siguientes planes:

- **PETI:** Plan de Seguridad, Privacidad y Tratamiento de Riesgos de la Información – EMSA.
- **SIPLAT:** Sistema Integral de Prevención y Control de Lavado de Activos y Financiamiento del Terrorismo.
- **GENERACIÓN DE INFORME DE PREMIOS.**

 Calle 51C Carrera 15B Barrio La Asunción.
Manizales, Colombia

 PBX: (606) 8841927

 www.loteriademanizales.com

 Línea de Atención al Cliente 018000423806






 emsa.loteriademanizales@gmail.com
loteriademanizales@une.net.co
notificacionesjudiciales@loteriademanizales.com



LOTERÍA DE MANIZALES

PARA GANARLA HAY QUE COMPRARLA

Planes transversales a las temáticas de Seguridad, Privacidad y Tratamiento de Riesgos de la Información – EMSA.

TEMÁTICA ARTICULADA	DESCRIPCIÓN	OBJETO	SISTEMA DE GESTIÓN DE CALIDAD
PETI:	Plan Estratégico de Tecnologías de la Información y las Comunicaciones	Formular los objetivos, planes e iniciativas que permitan la alineación y articulación de las TIC en la Lotería de Manizales y los objetivos estratégicos de la Entidad, para la vigencia, brindando soporte al cumplimiento de las funciones misionales acorde al marco de referencia de la arquitectura empresarial.	Código: GE-MA-03. Versión 01 Fecha de vigencia: 11/05/2023
PLAN DE SEGURIDAD, PRIVACIDAD Y TRATAMIENTO DE RIESGOS DE LA INFORMACIÓN.	Plan de Seguridad, Privacidad y Tratamiento de Riesgos de la Información – EMSA.	Describir las políticas de sistemas, anuncia los principales lineamientos en relación con aspectos generales de la informática con sistemas de información que apoyan la gestión administrativa, equipos de cómputo y seguridad informática.	Por asignación en el Sistema de Gestión.
SIPLAT:	Sistema Integral de Prevención y Control de Lavado de Activos y Financiamiento del Terrorismo.	El presente manual recopila la información relacionada con los elementos, normas, políticas y procedimientos que regirán el desarrollo del Sistema de Prevención y Control del Lavado de Activos y Financiación del Terrorismo, en cumplimiento de lo dispuesto por el CONSEJO NACIONAL DE JUEGOS DE SUERTE Y AZAR – CNJSA en el ACUERDO 317 DE 2016 y demás disposiciones normativas sobre la materia.	Instructivo: Manual SIPLAT Código: MER-IN-02. Versión: 01 Fecha de vigencia: 01/12/2022.
 Calle 51C Carrera 15B Barrio La Asunción. Manizales, Colombia	 PBX: (606) 8841927	 Línea de Atención al Cliente 018000423806	 emsa.loteriademanizales@gmail.com loteriademanizales@une.net.co notificacionesjudiciales@loteriademanizales.com
 www.loteriademanizales.com			



LOTERÍA DE MANIZALES

PARA GANARLA HAY QUE COMPRARLA

GENERACIÓN DE INFORME DE PREMIOS.

Reporte de información de ganadores de sorteo correspondiente a cada mes.

Cada mes se realiza la validación y reporte de las personas beneficiadas en cada sorteo, así mismo este reporte es validado y enviado a la Supersalud.

Instructivo: Cargue reportes UIAF
Código: MER-IN-01
Versión: 01
Fecha de vigencia: 01/12/2022.

El presente Plan de Seguridad, Privacidad y Tratamiento de Riesgos de la Información – EMSA, tiene articulación con los contenidos y alcances contemplados en los siguientes planes:

- **PETI:** Plan de Seguridad, Privacidad y Tratamiento de Riesgos de la Información – EMSA.
- **SIPLAT:** Sistema Integral de Prevención y Control de Lavado de Activos y Financiamiento del Terrorismo.
- **GENERACIÓN DE INFORME DE PREMIOS.**

Observacion: Cada uno de los planes descritos se encuentran publicados en la pagina de la Entidad www.loteriademanizales.com.

Se expide en Manizales, Caldas a los veinte y tres (23) días del mes de diciembre de 2023.

JORGE ANDRÉS ARTEAGA MARTÍNEZ
Gerente Emsa – Lotería de Manizales

Calle 51C Carrera 15B Barrio La Asunción.
Manizales, Colombia

PBX: (606) 8841927

www.loteriademanizales.com

Línea de Atención al Cliente 018000423806

emsa.loteriademanizales@gmail.com
loteriademanizales@une.net.co
notificacionesjudiciales@loteriademanizales.com