MANUAL Y POLITICA PARA LA SEGURIDAD INFORMATICA

EMPRESTUR S.A.S.
Nit. 811030670-5

Medellín, Antioquia

INTRODUCCIÓN

El manual y política para la seguridad informática representa una importante herramienta que servirá para garantizar el buen funcionamiento de los procesos tecnológicos, que contribuyen eficazmente en la optimización de los sistemas internos de la compañía, y garantizan la calidad en la gestión tecnológica con el fin de asegurar la seguridad de la información

Se definen las TIC de la compañía como la Tecnología de la Información y comunicaciones que permite a través de una serie de Hardware y Software establecer y garantizar las herramientas necesarias para determinar los métodos más aplicables que permiten retener, manipular, distribuir toda la información de Emprestur S.A.S., para ser aplicable por cualquier área, permitiendo la facilidad en tomar las decisiones en forma transparente y oportuna.

Con el Manual y política de seguridad informática, se pretende trazar los lineamientos bajo la responsabilidad del área de Tecnología de la Información, como de los usuarios del uso de esta, a fin de que toda administración en este contexto se realice de una manera clara, precisa y transparente, donde se respeten los parámetros establecidos en la política de uso y manejo de los equipos y herramientas tecnológicas.

La información es un activo de alto valor para Emprestur S.A.S., a medida que los procesos de la organización se hacen más dependientes de la información y de la tecnología que la soporta, se hace necesario contar con reglas de alto nivel que permitan el control y administración efectiva de los datos.

El presente manual contiene los lineamientos que rigen la actuación de los empleados o eventuales contratistas de Emprestur S.A.S, en cumplimiento de las disposiciones legales vigentes, con el objeto de salvaguardar la información.

Las políticas que aplican específicamente al personal de equipo de trabajo de informática se presentan en el numeral 2 del presente manual.

El manual de políticas contiene lineamientos y directrices tanto de seguridad de la información como de seguridad informática. La adopción de los dos enfoques busca afrontar integralmente las amenazas que pueden comprometer a la información de la entidad.

1. INDENTIFICACIÓN DE LA EMPRESA

EMPRESTUR S.A.S fue constituida el 16 de octubre de 2001, con su actividad laboral como empresa de transporte público de pasajeros en la modalidad especial

RAZÓN SOCIAL:	EMPRESTUR S.A.S
NIT:	811.030.670-5
DIRECCION:	Carrera 65 # 8B-91, C.C. Terminal del sur, locales 373, 374, 379, 380 y 381
SEDE PRINCIPAL:	Medellín
SEDES ALTERNAS o AGENCIAS:	Pereira y Manizales
TELEFONO:	3630203
ACTIVIDAD ECONOMICA:	Transporte Especial de pasajeros y de carga

2. DEFINICIONES

- **Amenazas:** cualquier acción o evento que puede ocasionar consecuencias adversas.
- **Ataques:** tipos y naturaleza de inestabilidad en la seguridad.
- **Autorización:** lo que se permite cuando se ha otorgado acceso.
- **Confidencialidad:** la información debe ser conocida exclusivamente por las personas autorizadas, en el momento y forma prevista.
- **Control de acceso:** limitar el acceso autorizado sólo a entidades autenticadas.
- **Controles:** cualquier acción o proceso que se utiliza para mitigar el riesgo.
- **Contra medidas:** cualquier acción o proceso que reduce la vulnerabilidad.
- **Estándar:** regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Sirven como especificaciones para la implementación de las políticas.
- **Evento de seguridad:** es la ocurrencia identificada de un estado del sistema, servicio o red, que indica una posible violación a la política de seguridad, una falla de las salvaguardas, o una situación desconocida que puede ser relevante para la seguridad.
- **Disponibilidad:** la información debe estar accesible y ser utilizable por los usuarios autorizados en todo momento, debiendo estar garantizada su propia persistencia ante cualquier eventualidad.
- **Impacto:** los resultados y consecuencias de que se materialice un riesgo.
- **Incidente de seguridad:** es toda aquella violación a las políticas de seguridad, fallas de los sistemas y pérdida del servicio, errores por datos incompletos e inexactos, fallas en procesos, violaciones a la confidencialidad e integridad de la información, entre otros.
- **Incidentes sobre virus:** es una ocurrencia simple de uno o varios archivos infectados por un virus en un computador o servidor. Cuando los virus reaparecen después de haberlos limpiado, se considerarán un nuevo incidente.
- **Integridad:** la información tiene que ser completa, exacta y válida, siendo su contenido el previsto de acuerdo con unos procesos predeterminados, autorizados y controlados.
- **Normas:** establecer los límites permisibles de acciones y procesos para cumplir con las políticas.
- **Políticas:** declaración de alto nivel sobre la intención y la dirección de la gerencia.
- **Vulnerabilidades:** deficiencias que pueden ser explotadas por amenazas.
- **Borrado seguro:** Procedimiento de eliminación de archivos que no permite la recuperación posterior de éstos.
- **Centro de Servicios Informáticos - CSI:** Equipo responsable de gestionar las solicitudes de servicio relacionadas con las plataformas de tecnologías de información Emprestur S.A.S.
- **Contratista:** Trabajador que hace parte de una empresa o entidad contratada por Emprestur S.A.S para la prestación de sus servicios.

- **Correo masivo:** Expresión usada en el presente manual de políticas para referirse a mensajes de correo electrónico enviado a múltiples destinatarios.
- **Criterio de seguridad informática en Emprestur S.A.S:** Conjunto de requisitos técnicos que deben considerarse para la planeación e implementación segura de infraestructura y aplicaciones de tecnología de información, así como para su posterior verificación.
- **Derechos / Privilegios de acceso:** Conjunto de permisos dados a un usuario o a un sistema para acceder a un determinado recurso (repositorio de red, aplicativo, datos).
- **Dispositivos móviles:** Son aparatos con algunas capacidades de procesamiento y de conectividad. Su principal característica es su movilidad. Los dispositivos móviles abarcan una gran variedad de equipos como: teléfonos inteligentes, tabletas, y computadoras portátiles.
- **Entidad:** Término que se usa en el presente documento para identificar Emprestur S.A.S cuando sea conveniente.
- **Equipos de trabajo de informática:** Expresión que se usa en el presente documento para identificar a los equipos de trabajo Emprestur S.A.S que son responsables de desarrollar, desplegar, mantener y administrar las plataformas de tecnología de información. Esta expresión abarca a los integrantes del área de sistemas y personal de otras áreas de la entidad con alguna de las responsabilidades mencionadas.
- **Equipo de seguridad de la información:** Grupo funcional adscrito a área de sistemas, cuya función primordial es la de gestionar la seguridad para el alcance previsto del SGSI, buscando que el nivel de riesgo de la información de la entidad permanezca en niveles aceptables.
- **Evento de seguridad informática:** Presencia identificada del estado de un sistema, servicio o red, que indica una posible violación de las políticas de seguridad informática, una falla de los controles, o una situación desconocida previamente que puede ser relevante para la seguridad.
- **Incidente de seguridad informática:** Un evento o serie de eventos de seguridad informática no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad informática. Todo incidente es un evento, más no todo evento es un incidente.
- **Manual de protección de la información:** Documento donde se establecen los lineamientos de seguridad para el manejo de la información en función de la clasificación de dicha información. Según la Política de identificación y protección de la información la información de la entidad se clasifica en Pública, Clasificada y Reservada.
- **Plataforma de tecnologías de información / Plataforma de T.I.:** Para propósitos del presente documento, las expresiones “plataforma de T.I.” y “plataforma de tecnologías de Información” hace referencia a todo el conjunto de recursos de tecnología de la información usados para generar, procesar, almacenar y transmitir información. Lo que incluye: sistemas de información, equipos de escritorio, portátiles, sistemas operativos, e infraestructura de red.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información:
- Confidencialidad: Propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Integridad:** Propiedad de mantener la exactitud y estado completo de la información, en otras palabras, proteger la información para que no sea adulterada o alterada de forma indebida.
- **Disponibilidad:** Propiedad de mantener la información disponible y utilizable cuando lo requiera un individuo, proceso o entidad autorizada.
- **Seguridad informática:** Rama de la seguridad de la información que se enfoca en la protección de la plataforma de tecnología de Información y de los datos que circulan, se procesan o almacenan en dicha plataforma.
- **Sistema de Gestión de Seguridad de la Información SGSI:** Sistema de gestión basado en un enfoque hacia los riesgos, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. El SGSI se rige por los requisitos de la norma internacional de gestión ISO/IEC 27001.
- **Software malicioso:** (También, código malicioso). Es un tipo de software que tiene como objetivo infiltrar o dañar un equipo de cómputo o sistema de información sin el consentimiento de su propietario. El software malicioso incluye virus, gusanos, troyanos, spyware, etc. El término “software malicioso” también hace referencia a software hostil o molesto.
- **Usuario:** Persona, proceso o aplicación de la entidad autorizada para acceder a la información o a los sistemas.
- **Cuentas de usuarios genéricas:** Es una cuenta destinada a representar un servicio, colectivo o evento que permite el acceso a distintos servicios.
- **Cifrado:** Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos.
- **Log’s:** es un registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema. Se utiliza en muchos casos distintos, para guardar información sobre la actividad de sistemas variados.
- **Sistemas de información críticos:** Son aquellos sistemas en los que un fallo puede ocasionar consecuencias graves en el entorno en el que está trabajando y producir perdida de información.
- **Llaves criptográficas:** Una clave, palabra clave o clave criptográfica es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa. En sistemas informáticos, la clave sirve para verificar que alguien está autorizado para acceder a un servicio o un sistema. Las claves también se utilizan en otros algoritmos criptográficos, como los sistemas de firma digital y las funciones de hash con clave (asimismo llamadas códigos de autentificación de mensajes).
- **Ofuscación de datos:** Se refiere a encubrir el significado de una comunicación haciéndola más confusa y complicada de interpretar.
- **Código fuente:** Es un programa informático (o software) es un conjunto de líneas de texto con los pasos que debe seguir la computadora para ejecutar dicho programa.

3. PROPÓSITOS

- Formalizar el compromiso Emprestur S.A.S frente a la seguridad informática.
- Definir los lineamientos de seguridad que deberán seguirse para proteger la información al interior Emprestur S.A.S.
- Fundamentar la futura definición de procedimientos, protocolos y estándares de seguridad informática.

4. PRINCIPIOS

Las políticas contenidas en el presente manual se justifican y sustentan en los principios de la seguridad de la información, tales principios son:

- Promover comportamientos de seguridad responsables.
- Promover las actuaciones profesionales y éticas.
- Promover cultura para la seguridad.
- Tener un enfoque basado en los riesgos.
- Buscar el cumplimiento de los requisitos legales y regulatorios pertinentes.
- Fomentar la mejora continua.
- Proteger la información clasificada.
- Evaluar las amenazas actuales y futuras de la información.
- Proteger la organización.
- Soportar el actuar de la entidad.
- Enfocarse en la organización.
- Ofrecer calidad y valor a las partes interesadas.
- Ofrecer información puntual y precisa sobre la gestión de la seguridad
- Concentrarse en aplicaciones organizacionales críticas.
- Buscar el desarrollo sistemas de información de forma segura.

5. ROLES Y RESPONSABILIDADES ASOCIADAS A LA PRESENTE POLÍTICA

Gestión de tecnología

- Formular y actualizar las políticas de seguridad informática para toda la entidad.
- Revisar, aprobar y procurar el cumplimiento de las políticas a través de la formulación y revisión de estas.
- Equipo directivo
- Hay que asegurar que el personal bajo su responsabilidad conozca, entiendan y atiendan las políticas contenidas en el presente manual.
- Aplicar controles o medidas que garanticen el cumplimiento de las políticas de seguridad informática dentro de los procesos del Sistema Integrado de Gestión.
- Alta Dirección

- Revisar y aprobar las políticas de seguridad informática de los empleados y/o contratistas Servidores públicos personal de apoyo y contratistas
- Conocer y cumplir las políticas indicadas en este manual.
- Informar y reportar los incumplimientos a la presente normativa en los distintos procesos de la entidad"
- Plantear e implementar las acciones correctivas y de mejora que se identifiquen en cada uno de los procesos.
- Informar y reportar los incumplimientos a la presente normativa en los distintos procesos de la entidad
- Apoyar a otros servidores en el cumplimiento de las políticas indicadas en este manual

Gerencia Administrativa y Financiera

- Dirigir el plan estratégico de seguridad de la información y tomar las decisiones que permitan gestionar la seguridad informática en el marco del cumplimiento de las políticas definidas y aprobadas.
- Identificar oportunidades para la mejora de las políticas de seguridad informática en función de las necesidades de la entidad y de los riesgos que sean identificados.

6. CUMPLIMIENTO DE REQUISITOS LEGALES Y REGULATORIOS

El presente manual de políticas fue construido para proteger la información y la plataforma de tecnologías de información de Emprestur S.A.S; en ningún momento la aplicación de las políticas de seguridad informática podrá atentar contra los derechos fundamentales de las personas como el derecho a la intimidad, a la vida, la salud o la seguridad.

7. SANCIONES Y PROCESO DISCIPLINARIO

- El desacato o incumplimiento a las presentes políticas por parte de un empleado o contratista de Emprestur S.A.S puede acarrear acciones disciplinarias. Dichas medidas se impartirán de acuerdo con la ley y al reglamento de trabajo de Emprestur S.A.S.
- Una infracción o falta de estas políticas por parte de un contratista puede generar la terminación de su contrato con Emprestur S.A.S.

8. POLÍTICA GENERAL DE SEGURIDAD INFORMÁTICA

La información es un activo estratégico para las operaciones diarias Emprestur S.A.S y a su vez un factor determinante para el éxito de su plan estratégico. Por ello, la Entidad está comprometida con la adopción de buenas prácticas de seguridad informática tendientes a implementar, mantener y mejorar su Sistema de Gestión de Seguridad de la Información SGSI.

Emprestur S.A.S espera el compromiso de todos sus servidores públicos y demás colaboradores de la entidad con el cumplimiento del presente Manual de Políticas.

8.1. Políticas para empleados y contratistas

Alcance

Estas políticas aplican tanto a los procesos realizados directamente por Emprestur S.A.S, como a los ejecutados a través de contratos o acuerdos con terceros.

Deben ser conocidas y cumplidas por los empleados, proveedores, contratistas y usuarios externos que hagan uso de la información de la entidad y de sus recursos tecnológicos.

Las políticas de seguridad informática también aplican para quienes se laboren en la modalidad de teletrabajo, siempre y cuando esta modalidad este aprobada.

El acceso remoto seria a través de una VPN (es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet), esta configuración permitiría el acceso a la red de la empresa de forma segura.

8.2. Políticas de identificación y protección de la información

Declaración principal:

Los activos de información dentro del alcance del SGSI de Emprestur S.A.S deben ser identificados, clasificados y definidos los responsables de cada uno de ellos.

- Identificación y clasificación de la información
- Los activos de información deben ser identificados y registrados en un inventario.
- Los activos de información deben tener propietario designado.
- El Propietario de un activo de información es responsable de:
- Definir los usuarios autorizados que pueden tener acceso al activo y sus privilegios de acceso.
- Determinar las clasificaciones correspondientes a la sensibilidad del activo.
- Hay que asegurar que se gestione el riesgo de seguridad del activo.
- Establecer las reglas de uso del activo, cuando sea necesario.
- Solicitar la aplicación de controles para la protección del activo de información.

- Cada activo de información debe tener un custodio designado, quien ha de protegerlo mediante la aplicación y el mantenimiento de los controles de seguridad autorizados por el propietario.

La información de Emprestur S.A.S se clasifica en:

- Información pública. Es toda información que Emprestur S.A.S genere, obtenga, adquiera, o controle.

- Información clasificada. Es aquella información que estando en poder o custodia de Emprestur S.A.S, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

- Información reservada. Es aquella información que estando en poder o custodia de Emprestur S.A.S, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 6 de marzo de 2014 (ley de transparencia y del derecho de acceso a la información pública nacional).

- El manejo de la información de Emprestur S.A.S debe seguir los lineamientos del Manual de Protección de la Información.

- Sólo se permite la transferencia de información Clasificada o Reservada cuando exista un acuerdo de confidencialidad o compromiso contractual que lo regule.

- Emprestur S.A.S tiene control total sobre la información que se almacene en la infraestructura de tecnología de la información de la entidad; por lo tanto, Emprestur S.A.S se reserva el derecho de mover, borrar, monitorear o tomar custodia de dicha información.

- Los empleados y contratistas son responsables de proteger la información de su trabajo y solicitar al área de gestión de la tecnología el almacenamiento seguro de la información cuya pérdida pueda causar incumplimientos legales y/o la interrupción de los procesos de la entidad.

8.3. Política de gestión del riesgo de seguridad informática

En Emprestur S.A.S la gestión de los riesgos fundamenta la toma de decisiones de seguridad informática.

- Lineamientos generales de la gestión del riesgo de seguridad informática
- Empleados y contratistas deben identificar y reportar condiciones que podrían indicar la existencia de riesgos de seguridad informática.

8.4. Política de gestión de incidentes de seguridad informática

En Emprestur S.A.S los eventos e incidentes de seguridad informática son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad.

- Reporte de eventos, incidentes y debilidades de la seguridad informática
- Los empleados y contratistas deben reportar inmediatamente al área de sistemas, todas las situaciones que puedan afectar la seguridad informática.
- La información específica sobre Incidentes o vulnerabilidades de seguridad informática, así como el detalle de las medidas para proteger las Plataformas de T.I., debe ser tratada como información Reservadas.

8.5. Política de uso adecuado de los recursos de la plataforma de T.I.

Toda la información de Emprestur S.A.S, así como los recursos para su procesamiento, almacenamiento y transmisión deben ser empleados únicamente para propósitos laborales o de la entidad; evitando su abuso, uso ilegal o desaprovechamiento.

- Requerimientos generales para el uso adecuado de la plataforma de T.I.
- Se prohíbe el uso de los recursos de plataforma de T.I. de Emprestur S.A.S para la realización de cualquier actividad ilegal.
- Para verificar el cumplimiento de las presentes políticas; Emprestur S.A.S podrá monitorear y auditar las Plataformas de T.I. de la entidad que son facilitadas a empleados y contratistas para el cumplimiento de sus deberes y funciones laborales.
- Los empleados y contratistas deben abstenerse de crear, acceder, almacenar o transmitir material ilegal, pornográfico, que promueva la violación de los derechos humanos o que atente contra la integridad moral de las personas o de las instituciones.
- Está prohibida la realización de pruebas a los controles de seguridad informática.
- No está permitido aprovechar las vulnerabilidades de seguridad de las plataformas de T.I.

8.6. Uso adecuado del correo electrónico

- No está permitido enviar correos masivos sin la autorización de la gerencia o las áreas de Talento humano o Comunicaciones.
- El área de sistemas y gestión tecnológica podrá establecer los límites en la cantidad de destinatarios y el tamaño de los mensajes de correo electrónico.
- No está permitido abrir los adjuntos de los correos sospechosos o que lleguen desde dominios desconocidos, que representan duda por su asunto en cuestión y que al abrirlo puede permitir ser vulnerables a un ataque critico de seguridad, se debe informar inmediatamente al área de TI para la revisión inmediata del adjunto.

8.7. Uso adecuado de equipos de cómputo asignados

No está permitida la instalación, ejecución y/o utilización de software diferente al preinstalado en los equipos de cómputo o al instalado por integrantes de los equipos de trabajo de informática.

- Los parámetros de configuración del sistema operativo solo deben ser modificados por integrantes de los equipos de trabajo de informática.
- Uso adecuado de servicios de red
- No deben almacenarse archivos personales en carpetas de la red.
- No se permite el uso de servicios de descarga o intercambio de archivos que funcionan bajo el esquema P2P.
- No está permitida la descarga de archivos de audio y/o video a menos que lo requieran en virtud de sus responsabilidades laborales.
- No está permitido deshabilitar o evadir los controles de navegación en internet.
- En horarios laborales, está prohibido acceder a páginas de transmisión de películas, programas de televisión y eventos deportivos.
- El acceso remoto a los equipos y dispositivos de la plataforma de T.I. solo está permitido para labores de soporte técnico autorizado.
- El acceso remoto a equipos de cómputo debe contar con la aprobación del empleado o contratista responsable de dicho equipo.
- Solo está permitido el uso de servicios de almacenamiento de información suministrados por la entidad.
- La red de visitantes está dispuesta únicamente para las personas que visitan temporalmente Emprestur S.A.S.

8.8. Uso de material protegido por derechos de autor

- El uso del software que es propiedad de Emprestur S.A.S es para el uso exclusivo de la entidad.
- Se prohíbe el almacenamiento de archivos multimedia (videos, música, imágenes o libros electrónicos) y cualquier otro tipo de contenido que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en las carpetas de red de la entidad.

- Se prohíbe el almacenamiento, uso, instalación y/o ejecución de software que viole las leyes y regulaciones vigentes de propiedad intelectual (derechos de autor y propiedad industrial) en la plataforma tecnológica de la entidad.

8.9. Manejo de dispositivos USB

Cuando se utilizan dispositivos móviles, se debe tener especial cuidado en garantizar que no se comprometa la información de Emprestur S.A.S. Se deberá tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo: Notebooks, Tablets, Ipads, Laptops, Teléfonos Celulares y sus tarjetas de memoria, dispositivos de almacenamiento removibles, tales como CDs, DVDs, USBs, Tapes, y cualquier dispositivo de almacenamiento de conexión USB.
Controles

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo pérdida, robo o hurto. En consecuencia, deberá entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

- Se deberán proteger física y lógicamente los dispositivos móviles propiedad de Emprestur S.A.S con el fin de evitar el hurto, acceso o la divulgación no autorizada de la información. En caso de ser necesario, se cifrará la información y se tendrán copias de respaldo.
- Emprestur S.A.S, con la información suministrada por área de TI brindará o denegará a los funcionarios, contratistas y terceros el acceso a la información o sistemas de información a través de los dispositivos móviles conforme los roles y responsabilidades.
- En caso de extravió o hurto de un dispositivo móvil asignado por Emprestur S.A.S, el funcionario, contratista o tercero será el responsable de informar el hecho de manera inmediata a la entidad, con el propósito de establecer las medidas de seguridad adecuadas y oportunas para la protección de la información contenida.
- Permanecer siempre cerca del dispositivo.
- No dejar desatendidos los equipos.
- Mantener cifrada la información clasificada.

Por otra parte, el responsable del dispositivo reportara en el menor tiempo posible cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información de Emprestur S.A.S, los que incluirán:

- Revocación de las credenciales afectadas
- Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.
- No abrir las memorias inmediatamente sean puestas en los equipos, se debe realizar primero un proceso de vacunación, para ellos se da clic derecho sobre el dispositivo USB y seleccionar la opción Scanear con Sophos Endpoint.

8.10. Política de personas y cultura frente a la seguridad informática

Se deben aplicar medidas de control antes, durante y después de finalizada la relación laboral, con el fin de mitigar los riesgos de seguridad informática asociados al factor humano.

- Antes del ingreso a laborar

Toda persona contratada, debe aceptar formalmente el cumplimiento de las políticas del presente manual.

- Durante la permanencia o la vigencia del contrato
  - Los empleados y demás colaboradores de Emprestur S.A.S son responsables por desempeñar sus funciones cumpliendo las políticas definidas en el presente manual.
  - Los empleados o demás colaboradores que tengan acceso a la información Emprestur S.A.S deben participar en las actividades de concientización y capacitación en materia de seguridad informática a las que sea convocado.
  - El incumplimiento de las políticas consignadas en el presente manual podrá generar acciones disciplinarias.
  - Las políticas de seguridad informática forman parte integral de los contratos de trabajo de los empleados.

- Terminación del contrato o cambio de cargo
  - Empleados y demás colaboradores que finalicen su relación laboral con la Entidad deben entregar a su superior inmediato o responsable, la información de la entidad que se encuentre bajo su responsabilidad y/o manejo como: informes, expedientes, correos electrónicos, comunicaciones internas y demás documentación generada en su estancia en la entidad.
  - La información y el conocimiento desarrollado por los empleados de Emprestur S.A.S durante el horario laboral y dentro de la vigencia del contrato laboral es propiedad de la entidad, por lo tanto, se prohíbe el borrado o la copia de dicha información por parte de empleados o demás colaboradores en proceso de retiro o por personal retirado.
  - Ante la finalización de la relación laboral o contractual de un empleado o demás colaboradores, se deben suspender inmediatamente los permisos de acceso a la plataforma de T.I. de la entidad.
  - El área de talento humano debe informar inmediatamente al área de Informática, los retiros o traslados de los empleados y demás colaboradores, con el fin de revocar o modificar los privilegios de acceso asignados ha dicho personal.
  - El superior inmediato del empleado y demás colaboradores es el responsable de gestionar el retiro o modificación de los derechos de acceso ante novedades laborales como la terminación o cambio del contrato.
  - El superior inmediato es el responsable de gestionar el respaldo de la información de los equipos de cómputo de los empleados y demás colaboradores en proceso de retiro.

8.11. Política de seguridad informática para contratación

La información de Emprestur S.A.S debe ser protegida en los procesos de contratación en todas sus etapas.

- Disposiciones generales
- Se deben designar servidores públicos de la entidad como supervisores de los servicios, funciones y contratos llevados a cabo por terceras partes.
- Los empleados y contratistas responsables por los servicios de contratistas o proveedores son responsables de identificar y valorar los riesgos de la información asociados al acceso de éstos.
- Los contratos celebrados entre Emprestur S.A.S y contratistas o proveedores con acceso a la información de la entidad, deben incluir cláusulas para mitigar riesgos de seguridad informática.
- Todos los proponentes invitados a un proceso de negociación o selección (contratistas o proveedores potenciales) deben firmar previamente un acuerdo de confidencialidad, siempre que dicho proceso implique la entrega de información Clasificada o Reservada de la entidad.

8.12. Política de seguridad física de la información y los equipos de cómputo

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.

- Seguridad en las instalaciones

- Fuera del horario laboral normal o cuando se alejen de sus lugares de trabajo, los empleados y contratistas deben bloquear el equipo y resguardar los datos, bien sean físicos (como documentos impresos y carpetas) o electrónicos (como memorias USB, Discos Duros Externos, CDs y DVDs).
- Cuando un empleado se percate de la presencia de personas sospechosas en las instalaciones de la entidad, debe reportar dicha situación.
- Cuando se imprima información clasificada o reservada, las impresiones deben ser retiradas inmediatamente.
- Las reuniones y sesiones de videoconferencias Emprestur S.A.S no deben ser grabadas en audio o video a menos que todos los participantes estén al tanto de la dicha grabación. En el acta de la reunión debe registrarse que la sesión fue grabada.
- No está permitido fumar, ingerir alimentos o bebidas en las salas o puestos de trabajo con equipos de cómputo.

- Seguridad de los equipos

  - Los empleados y demás colaboradores de Emprestur S.A.S son responsables de garantizar la debida protección de los equipos asignados (computadores de escritorio y dispositivos móviles) dentro y fuera de la entidad, lo que contempla (pero sin limitarse a) su vigilancia, el debido cuidado en su transporte y el uso de cualquier otra medida de seguridad física necesaria, en caso de pérdida o robo se debe adelantar el respectivo reporte.
  - Los equipos suministrados por Emprestur S.A.S, como computadores de escritorio y dispositivos móviles (incluye computadores portátiles), no deben ser objeto de alteraciones en su hardware. Toda modificación a los equipos debe ser autorizada y realizada por personal de soporte técnico de los equipos de trabajo de informática.
  - Se debe bloquear la sesión cuando el usuario se aleje del computador.
  - La salida de los computadores (de escritorio o portátiles) debe ser autorizada por el superior inmediato del empleado.
  - Toda pérdida de equipos de cómputo o de alguno de sus componentes, debe ser informada inmediatamente al área de sistemas.
  - Emprestur S.A.S no está obligado a prestar soporte técnico a equipos de cómputo que no sean propiedad de la entidad.
  - Los equipos de cómputo que no sean entregados por Emprestur S.A.S no deben conectarse a la red de la entidad, a menos que cumplan con los requisitos definidos y sean autorizados por el área de Informática.

8.13. Política de control de acceso a plataformas de tecnología de la información

Emprestur S.A.S otorga el nivel de acceso necesario a la información y su plataforma de T.I. para el cabal cumplimiento de las funciones empleados y demás colaboradores.

- Gestión de acceso a usuarios

  - Los administradores de los sistemas de información deben verificar que los privilegios de acceso de los usuarios en las Plataformas de tecnología de la información se han otorgado de acuerdo con la necesidad laboral legítima.
  - Los privilegios de acceso otorgados a los usuarios de las Plataformas de tecnología de la información deben ser autorizados por el superior inmediato o el supervisor respectivo.
  - Los privilegios de acceso otorgados a los usuarios de las Plataformas de Tecnología de Información deben ser revisados al menos anualmente por los jefes inmediatos de los usuarios.
  - No están permitidas las cuentas de usuarios genéricas para el ingreso a la Plataforma de T.I.
  - Todas las cuentas de usuario son personales e intransferibles.

- Empleados y demás colaboradores de Emprestur S.A.S deben reportar a su superior inmediato o al área de sistemas cuando tengan más derechos de acceso de los necesarios.
- A excepción de las carpetas de red, los usuarios deben abstenerse de ingresar a los servidores de la plataforma tecnológica Emprestur S.A.S, a menos que lo requieran en virtud de sus funciones laborales.
- En la eventualidad de requerirse el ingreso a un equipo o a alguna de las cuentas de los sistemas de información de la entidad asignadas a un empleado o colaborador ausente, el jefe directo será el único autorizado para solicitar el acceso.

- Manejo de contraseñas

- Los usuarios de las Plataformas de Tecnologías de la Información de Emprestur S.A.S deben abstenerse de escribir las contraseñas en medios físicos o electrónicos.
- Las contraseñas de acceso a las Plataformas de Tecnologías de la Información son personales e intransferibles, cada usuario es responsable de su uso y de preservar su confidencialidad.
- El préstamo de contraseñas está prohibido bajo cualquier circunstancia, en caso de hacerlo el usuario de la información responsable de la cuenta asume las consecuencias generadas por dicha situación.
- Los usuarios de las Plataformas de T.I. tienen la responsabilidad de cambiar su contraseña (o solicitar su cambio, si es el caso) en el evento que fuese revelada o existiese alguna sospecha de ello.
- Todos los usuarios de Las Plataformas de Tecnología de Información de la entidad deben emplear contraseñas seguras, es decir, que cumplan las siguientes características:

 7 caracteres como mínimo.
 Deben incluir letras mayúsculas y minúsculas.
 Deben incluir números.
 Deben incluir caracteres especiales, por ejemplo: !@#$%&*.
 No deben basarse en información personal como: fechas de cumpleaños, direcciones, números telefónicos, nombres de personas, números de documentos de identificación, nombre de la entidad, etc.
 No deben basarse en información de la entidad, es decir, no deben hacer referencia al nombre de la entidad, sus procesos, dependencias, áreas o funciones.

8.14. Política de operación de plataformas de tecnología de información

Emprestur S.A.S aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y Telecomunicaciones.

- Requisitos para la planeación y operación de las plataformas de T.I.
- Todas las adquisiciones de software y hardware deben estar avaladas técnicamente por el área de Informática.
- Los componentes y sistemas de la infraestructura de seguridad informática no deben ser inhabilitados, desviados, apagados o desconectados sin la previa autorización de la dirección Administrativa.

- Protección contra software malicioso
- No está permitido el ingreso intencionado de software malicioso a los equipos y redes de Emprestur S.A.S.
- La presencia identificada o sospechada de software malicioso debe ser reportada al área de sistemas.

- Intercambio de información
- Todo intercambio de información con terceras partes debe ser realizado de conformidad a lo dispuesto en el Manual de Protección de la Información.

8.15 Políticas de cifrado de la información

Deben aplicarse mecanismos de cifrado cuando exista un alto riesgo de comprometer la confidencialidad de la información clasificada o reservada de la entidad.

- Cifrado

o Empleados o contratistas que sean responsables de llaves (o claves) de cifrado deben reportar al Equipo de Seguridad de la información, novedades acerca del manejo de dichas llaves (por ejemplo: cambio de dueños, cambio de custodia, pérdidas, acceso no autorizado).

o Cada vez que se utilice el cifrado, los empleados y demás colaboradores no deben borrar la única versión legible de los datos, a menos que hayan probado que el proceso de des-cifrado puede restablecer una versión legible de los datos.

o Se deben utilizar mecanismos de cifrado cuando se requiera el almacenamiento de información reservada o clasificada en medios removibles (como memorias USB, discos duros externos, CD y DVD).

o Se deben utilizar mecanismos de cifrado cuando se requiera enviar información reservada o clasificada a través de correo electrónico.

8.16 Política de dispositivos móviles

El acceso a los datos y sistemas de información de Emprestur S.A.S a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad informática.

- Computadores portátiles

o Los usuarios que tengan bajo su responsabilidad computadores portátiles de Emprestur S.A.S son responsables de su protección dentro y fuera de las instalaciones de la entidad.
o Los usuarios de computadores portátiles de Emprestur S.A.S deben emplear medidas de seguridad para su adecuado manejo fuera de las instalaciones de la entidad. Las medidas de protección incluyen, pero no se limitan a:
 Llevar los computadores portátiles como equipaje de mano en viajes terrestres y aéreos.
 Mantener a la vista y vigilar el computador portátil en todo momento que se esté fuera de las instalaciones de la entidad o de la vivienda del empleado.
 Ocultar el computador portátil de la vista de personas externas cuando se esté transportando en un vehículo.
o Los computadores portátiles están cubiertos por la sección “Seguridad física de los equipos” del presente manual de políticas.

• Dispositivos móviles diferentes a computadores portátiles Nota: esta sección hace referencia a dispositivos como teléfonos móviles inteligentes y tabletas.
o Los usuarios de dispositivos móviles entregados por Emprestur S.A.S son responsables de su protección dentro y fuera de las instalaciones de la entidad.
o Los usuarios de dispositivos móviles entregados por Emprestur S.A.S deben abstenerse de modificar las configuraciones de seguridad de dichos dispositivos.
o Los usuarios de dispositivos móviles entregados por Emprestur S.A.S deben reportar inmediatamente el robo o pérdida de dicho dispositivo al personal de los equipos de trabajo de informática.
o No está permitido el envío de información Clasificada o Reservada a través de servicios de mensajería instantánea no institucionales (como WhatsApp, Telegram, etc.).
o Emprestur S.A.S no está obligado a prestar soporte técnico a dispositivos móviles que sean de propiedad de los usuarios o cualquier otro que no sea propiedad de la entidad.
o Los usuarios que accedan a los servicios de la plataforma de T.I. (por ejemplo, al correo electrónico) a través de un dispositivo móvil propio, deben reportar inmediatamente el robo, cambio o pérdida de dicho dispositivo al área de sistemas.

8.17. Política de cumplimiento

Emprestur S.A.S cumple la regulación y legislación vigente aplicable en materia de seguridad informática.
• Cumplimiento legal y normativo
o Será sancionado con las acciones disciplinarias y legales correspondientes, al que utilizare registros informáticos, software u otro medio para ocultar, alterar o distorsionar información requerida para una actividad de la entidad, para el cumplimiento de una obligación respecto al Estado o para ocultar los estados contables o la situación de un proceso, dependencia o persona física o jurídica.
o Toda la información de ciudadanos o servidores públicos y contratistas que incluya cédulas de identidad, datos de contacto o información financiera debe ser sólo accesible al personal de la entidad que necesite ese acceso en virtud de su trabajo.
o La realización de auditorías (verificaciones o pruebas de seguridad) no deben afectar la normal operación de los sistemas de información o plataformas.

9. POLÍTICAS PARA EL PERSONAL DE LOS EQUIPOS DE TRABAJO DE INFORMÁTICA

Alcance
Estas Políticas aplican exclusivamente a personal de los equipos de Informática de Emprestur S.A.S ya sea interno o externo, en el ámbito del proceso de Planeación y Administración de las TIC.

9.1. Política de gestión del riesgo de seguridad informática

En Emprestur S.A.S, la gestión de los riesgos fundamenta la toma de decisiones de seguridad informática.

- Lineamientos generales de la gestión del riesgo de seguridad informática
  - Se deben identificar los riesgos a los que se encuentran expuestos los activos de información de la entidad.
  - Los criterios de evaluación y aceptación de riesgos de seguridad informática deben estar alineados con los criterios y políticas de gestión del riesgo de la entidad.
  - Los riesgos de seguridad informática analizados deben ser objeto de tratamiento (mitigar, transferir, evitar, aceptar), dicho tratamiento debe ser coherente con los criterios de aceptación de riesgos.
  - Los riesgos deben ser monitoreados después de su tratamiento para asegurar que siguen estando en niveles aceptables para la entidad.
  - En los casos que se realice la estimación económica de los riesgos, se debe asegurar que el valor de la aplicación de medidas de mitigación sea inferior al costo de las consecuencias de la materialización de los riesgos.

9.2. Política de gestión de incidentes de seguridad informática

En Emprestur S.A.S los eventos e incidentes de seguridad informática son gestionados oportunamente con el fin de minimizar el impacto sobre la entidad.

- Gestión de los Incidentes de seguridad informática
  - Debe conformarse y mantenerse un equipo multidisciplinario (directivos) para la respuesta y tratamiento a los incidentes de seguridad informática.
  - La atención de incidentes debe seguir los procedimientos de Atención de Acciones preventivas o Atención de acciones Correctivas, para esto existe la plataforma GLPI donde los funcionarios generan sus tickets, dependiendo del incidente presentado.

9.3. Política de seguridad informática asociada a contratistas

La información de Emprestur S.A.S debe ser protegida de los riesgos generados por el manejo o acceso de contratistas y proveedores.

- Requisitos de seguridad informática asociados a contratistas y terceros
  - El acceso de contratistas y proveedores a información o a plataformas de tecnología de Información de Emprestur S.A.S, se concede solamente cuando se demuestre la necesidad de su uso y esté expresamente autorizado por el propietario o superior inmediato de los activos de información o sistema de información respectivo.

o Únicamente debe concederse acceso remoto a plataformas de tecnología de Información a clientes, contratistas y proveedores, cuando estos tengan una necesidad legítima que lo justifique. El acceso remoto debe limitarse al tiempo requerido para cumplir con las actividades, debe ser autorizado por el propietario del activo respectivo o superior inmediato y posteriormente gestionado por personal autorizado del área de sistemas.
o El tercero que ejerza funciones de administración y soporte de sistemas de información, debe garantizar que se generan registros automáticos (Log's de auditoría) de dichas labores.

9.4. Seguridad física de la información y los equipos de cómputo

Se debe brindar seguridad física a la información de la entidad y a los recursos de la plataforma de T.I., de modo que se encuentren en condiciones ambientales adecuadas y a su vez, sean protegidos de situaciones como acceso no autorizado, robo, destrucción o desconexión.

• Zonas restringidas de procesamiento

o Se deben identificar y especificar las zonas restringidas de procesamiento de Emprestur S.A.S destinadas a alojar equipos y dispositivos de la plataforma de T.I. de la entidad.
o Todo sistema, equipo, dispositivo, o medio crítico para la transmisión, procesamiento y almacenamiento de la información de Emprestur S.A.S debe ser ubicado dentro del centro de cómputo (rack). Si no se pudiera ubicar algún equipo dentro de estas zonas, dicho equipo debe ser objeto de controles complementarios de acceso físico.
o Sólo personal autorizado puede ingresar a dicha zona.
o En el caso particular del centro de cómputo, se debe generar y mantener registro de los accesos de personal tanto interno como externo. El periodo de retención para estos registros es de un año como mínimo.
o El personal no autorizado interno o externo sin acompañamiento dentro de las zonas restringidas de procesamiento debe ser retirado de dicho lugar y además debe reportarse.
o Los privilegios de acceso a las zonas restringidas de procesamiento deben ser revisados al menos cada trimestre.
o Las zonas restringidas de procesamiento deben estar dispuestas para brindar condiciones ambientales adecuadas (como temperatura y humedad) para mantener de forma óptima los recursos y la información allí alojados.

• Seguridad física de los equipos

o Siempre que se reutilice un servidor, computador portátil o un computador de estación de trabajo, se requiere la realización previa de un Borrado Seguro de la información almacenada en dichos equipos antes que sean entregados a los nuevos usuarios.
o Debe realizarse Borrado Seguro de los equipos de forma previa al proceso de disposición final (por ejemplo: venta, donación o destrucción).
o Los servidores deben estar ubicados de modo que se reduzcan los riesgos generados por amenazas del entorno (es decir, evitando daños derivados de situaciones como manifestaciones sociales, inundaciones, humedad o incendio).
o Todos los equipos de procesamiento críticos deben tener controles para evitar caídas de la plataforma de TI causadas por fallas en el servicio eléctrico.

9.5. Control de acceso a plataformas de tecnología de la información

Emprestur S.A.S otorga el nivel de acceso a la información necesario para el cabal cumplimiento de las funciones.

- Proceso de control de acceso
  - El control de acceso es una característica indispensable para las plataformas de tecnología de la información.
  - Todo proceso de control de acceso debe tener un responsable de su gestión.
  - La gestión del proceso de control de acceso debe comprender las actividades de solicitud, aprobación, asignación, modificación y revocación del acceso.
  - Cuando aplique, las medidas de control de acceso a las plataformas de tecnología de la información deben cumplir el Criterio de seguridad informática.
  - El acceso remoto a plataformas de tecnología de la información de Emprestur S.A.S debe ser autorizado por los administradores de las plataformas respectivas.
  - El acceso remoto a plataformas de tecnología de la información debe ser realizado a través de VPN u otros medios que garanticen la seguridad en la comunicación.

- Gestión de acceso a usuarios
  - Las cuentas de administración de las Plataformas de tecnología de la información sólo deben ser usadas cuando sea necesario dicho privilegio, esto indica que son necesarios esos privilegios de administrador para realizar una labor como la instalación de un aplicativo o la asignación de un permiso especial para realizar un proceso que necesita de privilegios elevados.

- Manejo de contraseñas
  - Los nombres de usuario y contraseñas se rigen por el Criterio de seguridad informática de Emprestur S.A.S.
  - Las contraseñas de administración de las Plataformas de tecnología de la información podrán ser escritas en medios físicos o electrónicos únicamente si son objeto de medidas de seguridad física y/o lógica, según lo establecido en el Criterio de seguridad informática de Emprestur S.A.S.

9.6. Operación de tecnologías de información y comunicaciones

Emprestur S.A.S aplica controles para el funcionamiento correcto y seguro de las Plataformas de tecnología de la información y Telecomunicaciones.

- Requisitos para la planeación y operación de las Plataformas de tecnología de la información
  - Las nuevas plataformas o soluciones de tecnologías de la información deben ser analizadas en la fase de planificación con el fin de identificar los requisitos funcionales y de seguridad informática.
  - Las Plataformas Tecnológicas de la Entidad deben ser configuradas de conformidad con el Criterio de seguridad informática de Emprestur S.A.S.
  - La realización de auditorías, verificaciones o pruebas de seguridad informática no deben afectar la normal operación de las Plataformas de tecnología de la información.

- Protección contra software malicioso y móvil

o La plataforma de T.I de Emprestur S.A.S debe ser objeto de protección frente software malicioso.

• Respaldo de la información

o La información importante de la entidad alojada en los repositorios de red y los sistemas de información críticos deben ser respaldados a intervalos programados.

o Los respaldos de información deben ser probados regularmente, para verificar que la información si es recuperable ante un incidente.

o Los respaldos de información deben almacenarse además en un lugar externo a la sede de Emprestur S.A.S, evitando que, ante la posibilidad de un desastre al interior de la misma, se pierda por completo la información.

• Intercambio de información

o Las direcciones IP internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser considerados y tratados como información clasificada.

o La creación de una conexión directa entre las Plataformas de tecnología de la información y las organizaciones externas a través de Internet o cualquier otra red pública, debe estar autorizada por el Área de sistemas.

2.7 Adquisición, desarrollo y mantenimiento de sistemas de información

Los aplicativos de Emprestur S.A.S deben ser asegurados en sus fases de planeación, adquisición, desarrollo, implementación y operación.

• Requerimientos de seguridad de los sistemas de información

o Durante la etapa de definición de requisitos para desarrollar, adquirir o modificar un aplicativo, se deben especificar claramente todos aquellos requisitos concernientes a la seguridad. Debe existir un registro que evidencie la documentación de tales requisitos.

o Los requisitos de seguridad de los aplicativos deben incorporar los lineamientos del Criterio de seguridad informática aplicables o aquellos que sean definidos por la gerencia.

o La contratación de un desarrollo a medida, adquisición de software o sistemas de información debe incluir entrenamiento en administración de las funciones de seguridad de dichas aplicaciones.

o La contratación de un desarrollo a medida, adquisición o modificación de software o sistemas de información debe incluir la entrega de la documentación y la transferencia de conocimiento técnico y operativo suficiente al personal de soporte de Emprestur S.A.S.

o Deben definirse requisitos previos a la contratación de proveedores de desarrollo o soporte de software y sistemas de información que incluyan:

 Aseguramiento de la disponibilidad y continuidad del servicio.

 Condiciones para la entrega de código fuente (por ejemplo: ante el incumplimiento del proveedor) cuando el código fuente no sea propiedad de la entidad.

 Acuerdos de niveles de servicio (ANS) adecuados a la criticidad de la aplicación desarrollada o soportada por el proveedor.

 Requisitos de seguridad.

 La realización de verificaciones de la seguridad a la aplicación; ya sean estas auditorías al código fuente o pruebas de seguridad.

- Gestión de vulnerabilidades técnicas
  - Se debe verificar que el procesamiento del aplicativo es correcto, tanto en ambiente de pruebas como de producción, así como el cumplimiento de los requisitos definidos en la etapa de planeación
  - Las vulnerabilidades técnicas de las Plataformas de tecnología de la información deben ser objeto de un procedimiento de gestión orientado a la remediación de dichas vulnerabilidades.

- Cifrado
  - Los controles de cifrados empleados en la entidad deben seguir los requerimientos del Criterio de Seguridad Informática de Emprestur S.A.S.
  - Las llaves criptográficas deben tener un custodio designado.
  - Se debe mantener un inventario de las llaves criptográficas que son responsabilidad de informática.

- Seguridad de los archivos del sistema
  - El personal de desarrollo de sistemas de información no debe tener facultad para trasladar o modificar software al ambiente de pruebas ni al ambiente de producción, este proceso se debe hacer en compañía del área de sistemas.
  - A menos que se obtenga un permiso por escrito del propietario de la información (superior inmediato o supervisor de las bases de datos) toda prueba a sistemas de información (o a funcionalidades de estos) diseñados para manejar información reservada o clasificada:
    - Debe llevarse a cabo con datos que no sean clasificados o reservados
    - Deben emplearse soluciones de ofuscación de datos, que impidan la correlación de la información por parte de eventuales atacantes.
  - Sólo el personal responsable del desarrollo de software debe tener acceso al código fuente o en su defecto el administrador del área de informática.

9.8. Dispositivos móviles

El acceso a los datos y sistemas de información de Emprestur S.A.S a través de dispositivos móviles debe ser realizado de forma regulada y controlada con el fin de evitar incidentes de seguridad informática.

Computadores portátiles

Los computadores portátiles de la entidad deben tener instalada una herramienta de cifrado de datos que impida la fuga de información en caso de robo, pérdida o intentos de acceso no autorizado al equipo.

10. POLÍTICAS DE BACKUP

Estas Políticas aplican exclusivamente a los procesos de bases de datos, imágenes digitalizadas, información y servidores virtuales, además de otros datos que se procesan en los servidores, para el óptimo desempeño de los aplicativos, los cuales debemos custodiar y proteger en Emprestur S.A.S tanto a nivel interno como externo, en el ámbito de Planeación y Administración de las TIC

10.1. Backup

El acceso a los datos y sistemas de información garantizan la estabilidad en los procesos a diario, pero estos deben estar respaldados para prevenir posibles desastres informáticos los cuales se encuentran programados de forma controlada con el fin de evitar incidentes de seguridad y perdida de la información, además llegado a suceder un incidente grave se pueda realizar la restauración de la información de forma segura y sin perdida alguna o mínima ocurrido el caso.

- Bases de datos.

Este proceso de Backup o respaldo de bases de datos lo realiza el software Veeam Backup Communitiy Edition, los servidores que poseen motor de base de datos están realizando una copia incremental cada 24 horas de la información, en este sentido se estaría perdiendo un día de información en caso de desastre o incidente.
También se genera un Backup diario en el hosting VPS de Emprestur S.A.S como segunda medida de contingencia en pos de la seguridad de la información.

- Backup de archivos e imágenes

Este proceso de Backup o respaldo de documentos e imágenes, sistema de gestión documental Digitallogic, estas imágenes digitalizadas reposan en una unidad de almacenamiento, se encuentra en un servidor con Windows Server 2019 y lo realiza el software Veeam Backup Communitiy Edition, esta copia es granular y se ejecuta cada 24 horas, en este sentido se estaría perdiendo en caso de desastre o incidente información de un día.

- Backup externos.

Los Backup externos se utilizan como segunda medida de contingencia, se utiliza el servidor hosting VPS de Emprestur S.A.S se realiza una copia diaria de bases de datos y semanalmente las bases de datos y demás archivos de las aplicaciones. Esta información se guarda comprimida y encriptada.

- Backup servidores físicos y virtuales.

Este Backup incluye 1 servidor virtual SRVEMPRESTURV que se utiliza para el monitoreo de las cámaras de los vehículos asignados al contrato de ISAGEN y 2 servidores físicos. Este Backup se genera cada 24 horas.

11. POLÍTICAS TELEFONÍA IP

Estas Políticas aplican exclusivamente a los procesos con la telefonía IP, donde se diseñan procedimientos de seguridad que garanticen la disponibilidad, calidad e integridad de los datos; Para proteger estos, tanto a nivel interno como externo en Emprestur S.A.S.

11.1. Telefonía

El acceso a los datos y sistemas de información de Emprestur S.A.S garantizan la estabilidad en nuestros procesos a diario, pero estos deben estar respaldados por posibles desastres informáticos, para lo cual se realizan de forma controlada estos, con el fin de evitar incidentes de seguridad y perdida de la información, además la planta permite realizar seguimiento completo de las llamadas salientes y entrantes en todos sus niveles.

- Llamadas internas.

Este tipo de llamadas se generan a nivel interno y tienen como objetivo la comunicación y ubicación entre los funcionarios (extensiones) de Emprestur S.A.S, para realizar estas llamadas basta con indicar la extensión y marcar la tecla llamar para realizar la comunicación deseada.

- Llamadas locales.

Este tipo de llamadas se dan en el ámbito local, o sea, en la ciudad en que nos encontramos y a nivel del municipio y tienen como objetivo la comunicación y ubicación de personal externo, clientes o proveedores; con fines laborales. Para realizar estas llamadas basta con marcar el número fijo con el cual se realizará la comunicación, luego de esto el funcionario debe oprimir la tecla llamar para realizar la comunicación.

- Llamadas nacionales y a celulares.

Este tipo de llamadas se dan en el ámbito nacional, tienen como objetivo la comunicación y ubicación de personal externo (clientes y proveedores), con fines laborales. Para realizar las llamadas nacionales y a celulares, cada funcionario tiene un clave que es intransferible, basta con indicar el número con el cual se realizará la comunicación, luego de esto el funcionario debe marcar la clave asignada la cual es solicitada desde la planta telefónica, además de oprimir la tecla llamar para realizar la comunicación deseada

12. POLÍTICAS CÁMARAS DE VIGILANCIA

Estas Políticas aplican exclusivamente a los procesos de vigilancia a través de las cámaras, donde se diseñan procedimientos de seguridad que garanticen la disponibilidad, calidad e integridad de los datos; Para proteger estos tanto a nivel interno como externo.

12.1. Cámaras de vigilancia

El acceso a los datos y sistemas de información de Emprestur S.A.S garantizan la estabilidad en nuestros procesos, estos están respaldados ante posibles desastres informáticos, con el fin de evitar incidentes de seguridad y perdida de la información, además el servidor guarda por un 20 días los videos para permitir realizar seguimiento

completo de cualquier movimiento o novedad sospechosa en todos sus niveles, con el objetivo de preservar la seguridad y armonía en Emprestur S.A.S.

- Visualización y seguimiento de las cámaras.

La visualización de las cámaras las puede realizar las personas autorizadas por la gerencia. Las cámaras están configuradas para realizar grabación en todo momento que se detecte movimiento

- Grabación y videos cámaras.

Se cuenta con 30 cámaras situadas en puntos estratégicos, la grabación de las cámaras se realiza 24/24, 7/24 los 365 días del año, estas se encuentran programadas para almacenar hasta 20 días lo que quiere decir que las grabaciones que llegan al día 20 van siendo eliminadas para dar espacio a las que van entrando con fechas actuales, están configuradas para grabación por movimientos detectados.

- Configuración y solicitud de videos cámaras.

La configuración y administración del sistema se encuentra bajo la responsabilidad del área de sistemas de Emprestur S.A.S, la solicitud de videos se realiza al área de sistemas por parte de la gerencia o el área jurídica, ninguna otra área o funcionario puede autorizar la generación de videos o grabaciones para cualquier fin, además estas solicitudes deben ser realizadas por correo con el fin de llevar un control de los videos solicitados, se aclara que cuando se trata de videos que aportan evidencia a situaciones administrativas y que servirán como prueba en eventuales procesos disciplinarios, penales o fiscales, estos se custodian en una ruta especifica donde se mantienen guardados y con su respectiva copia, para que estén disponibles en el momento que se soliciten.

13. POLÍTICAS SISTEMA CONTRA INCENDIOS

Estas Políticas aplican exclusivamente a los procesos del sistema contra incendios, donde se diseñan procedimientos de seguridad que garanticen la disponibilidad, calidad e integridad de los datos; para proteger estos, tanto a nivel interno como externo en Emprestur S.A.S.

13.1. Sistema contra incendios

Emprestur S.A.S cuenta con un sistema contra incendios que ayuda a evitar incidentes o lesiones a empleados o visitantes y perdida de la información, para contrarrestar esto se tienen extintores de acción manual que permiten mitigar cualquier posible incendio.

14. POLÍTICAS SISTEMA DE IMPRESIÓN

Estas Políticas aplican exclusivamente a los procesos de impresión, donde se diseñan procedimientos de seguridad que garanticen la disponibilidad, calidad e integridad de los datos; Para proteger estos tanto a nivel interno como externo en Emprestur S.A.S.

14.1. Sistema de impresión

El acceso a los datos y sistemas de información garantizan la estabilidad en los procesos diarios, por ello, el interés por reorganizar los procesos documentales está favoreciendo la implantación de políticas de impresión. Su puesta en marcha tiene como objetivo disminuir la inversión en este apartado, así como mejorar los métodos de trabajo para que

los empleados desempeñen sus funciones con mayor eficiencia y eficacia, con el objetivo de preservar la seguridad, además de ayudar con el medio ambiente, favoreciendo al planeta.

- Configuración del sistema de impresión.

Emprestur cuenta con 4 impresoras láser conectadas en red, 2 de ellas en modalidad de arrendamiento, actualmente se utiliza el software de KYOCERA Net Viewer que permite controlar lo siguiente:

o Control y gestión de impresión: Registro de los trabajos de impresión, control por usuario.

o Análisis del uso de impresoras: Informes detallados para analizar el uso de impresión.

o Pin para cada usuario, este le permite realizar el trabajo de impresión, escaneo y copia.

- Seguimiento al sistema de impresión.

KYOCERA Net Viewer Registra las operaciones de impresión y proporciona en tiempo real registros detallados de la actividad de las impresoras. Entre la información proporcionada se encuentran:

o Fecha y hora de la impresión,

o nombre del usuario que realizó la impresión,

o número total de páginas,

Los datos de impresión están disponibles en formato CSV y Excel para usuarios expertos.

15. POLÍTICAS SISTEMAS PROPIOS

Estas políticas aplican tanto a los procesos realizados directamente por Emprestur S.A.S, como a los ejecutados a través de contratos o acuerdos con terceros.

Deben ser conocidas y cumplidas por los empleados, proveedores, contratistas y usuarios externos que hagan uso de la información de la entidad y de sus recursos tecnológicos en las siguientes ubicaciones:

Las políticas de seguridad informática también aplican para los empleados que llegaran a acogerse en la modalidad de teletrabajo, siempre y cuando esta modalidad este aprobada.

OBJETIVO: Definir las herramientas para hacer desarrollos (Base de Datos y Lenguaje de Programación), así como la forma para realizar los cambios y mantenimiento a dicho software.

ALCANCE: Esta Política aplica a todos los Usuarios de las aplicaciones de Emprestur S.A.S y/o contratistas involucrados en el desarrollo, actualización y pruebas de programas, así como en la seguridad a los mismos.

RESPONSABLES: Ejecución / Cumplimiento: Desarrollador
Gestión / Administración: Área de Sistemas Control / Seguimiento: Área de Sistemas

15.1. Gestión de sistemas propios

Los activos de información dentro del alcance del SGSI de Emprestur S.A.S deben ser identificados, clasificados y definidos los responsables de cada uno de ellos.

15.1.1. Proyectos de Desarrollo.

a) Para todo desarrollo de Software en la entidad, o para cumplimiento de proyectos especiales que involucren aplicaciones o sistemas de información, el Área de Sistemas, debe diseñar los formatos necesarios para documentar las siguientes actividades:
i) Un análisis de requerimientos internos, que debe ser revisado y aprobado por el Desarrollador.
ii) Un documento RFI – Requerimiento de Información, para entrega al Desarrollador.
iii) Un análisis técnico de requerimientos, como respuesta por parte del Desarrollador.
iv) Un documento RFP - Requerimiento de Propuesta, para entrega al Desarrollador.
v) Un documento Propuesta, que debe contemplar: Análisis situacional, matriz de riesgos del proyecto, propuesta económica, propuesta técnica, documentación legal y jurídica, demás soportes requeridos acordes al cada proyecto.

15.1.2. Ciclo de vida de desarrollo de software.

a. Debe definirse y aplicarse una metodología de desarrollo de aplicativos que contemple como mínimo las siguientes fases:
i) Concepción / análisis de negocio: Se debe exigir para todo desarrollo de Software, un levantamiento de información, un análisis situacional y deben estar claramente documentadas.
ii) Planeación y diseño: debe contemplar un diseño de la solución, y un plan de ejecución.
iii) Desarrollo: debe especificar las herramientas de desarrollo, la estructura y arquitectura de la solución, modelos entidad-relación y diccionarios de datos.
iv) Prototipo y pruebas: Debe contemplar la presentación de prototipos de evaluación y ajuste.
v) Instalación y estabilización: Debe contemplar plan de implementación, migración y estabilización de la solución.
vi) Soporte y mantenimiento: debe contemplar el plan de mantenimientos correctivos, Niveles de Acuerdo de Servicios y plan de continuidad de la solución que incluya plan de respaldo, plan de recuperación y plan de contingencia. Para cada solución se deben entregar: Manual de Usuario, Manual de administración, Manual Técnico de Instalación y configuración.

15.1.3. Ambientes de trabajo.

a. Para la adecuada gestión de proyectos de desarrollo, mantenimientos, pruebas e implementaciones, el Área de Sistemas debe implementar la infraestructura mínima de seguridad que garantice la adecuada gestión y control de los proyectos de software, implementando con los recursos existentes, los siguientes ambientes tecnológicos:

i. Ambiente de desarrollo: configuración orientada a la generación de desarrollos, en el cual los desarrolladores crean y modifican los objetos a solicitud del área Responsable de la Información.
ii. Ambiente de Pruebas / Testing: configuración orientada a la generación de pruebas por parte del Área de Sistemas y por el usuario, replica del ambiente de producción en donde se realizarán todas las pruebas necesarias para garantizar el buen funcionamiento de los aplicativos.
iii. Ambiente de Producción: configuración orientada al usuario final, ambiente donde se realiza el procesamiento real de la información utilizada para la toma de decisiones.

b. Para cada ambiente debe existir una configuración independiente en Sistema Operativo, Base de Datos y aplicación

15.1.4. Ambientes de prueba.

a. Debe existir un procedimiento de pruebas a programas que defina actividades y responsables.
b. Debe definirse un plan de pruebas que especifique escenarios de pruebas, niveles y tipos de pruebas que se deban realizar a los aplicativos.
c. Los datos del ambiente de pruebas deben ser una réplica del ambiente de producción.
d. El resultado de las pruebas debe documentarse por los desarrolladores en conjunto con los usuarios del área solicitante.

15.1.5. Ambientes de producción.

a. El Área de Sistemas debe Integrar y mantener todas las actividades de gestión de cambios (documentación y formación procedimental para usuarios y administradores) del Software / aplicaciones.
b. Debe disponerse de un inventario de aplicativos actualmente existentes en Emprestur S.A.S, especificando si se encuentran en producción o desarrollo, si ha sido un desarrollo propio o adquisición a terceros.
c. Para todos los cambios y ajustes autorizados, y en ejecución se debe conservar un registro escrito de las modificaciones realizadas, para la cual se debe crear un registro de control de cambio.
d. Los cambios de emergencia deben ser debidamente aprobados, auditados y documentados.
e. Todo cambio a los aplicativos debe ser solicitado por el jefe del área usuaria, y aprobado por el Área de Sistemas. Si se requieren cambios a los datos, deben ser aprobados por el responsable de la Información y se debe crear un formato de cambios de información.
f. Debe existir un procedimiento para la solicitud, autorización y aprobación para todos los cambios a aplicativos.
g. La documentación de todas las aplicaciones de Emprestur S.A.S debe ser permanentemente actualizada por los desarrolladores.

15.1.6. Ambientes de seguridad.

a. El Área de Sistemas debe implementar los mecanismos y herramientas necesarias para garantizar la seguridad en los procedimientos y métodos de desarrollo, operaciones y gestión de cambios del Software / aplicaciones, que se desarrollen interna o externamente, para la entidad.
b. Todos los Sistemas de Información deben contar con usuario y clave (Fuerte) la clave debe estar encriptado.
c. Todos los Sistemas de Información deben permitir restringir el acceso a las opciones de la aplicación utilizando para ello, los perfiles de acceso.
d. Los perfiles de acceso deben ser de acceso restringido, tan solo el administrador del Sistema de Información debe tener acceso a los mismos.
e. Todas las aplicaciones deben tener pistas o registros de auditoría (al menos para los datos críticos), en el cual se pueda identificar quien ha realizado cambios, borrados o inserción de datos no autorizados.
f. Las pistas de auditoría no deben permitir cambios de las mismas (son únicamente de lectura).
g. El software debe permitir realizar Copias de Seguridad de las pistas para así, borrar y reducir el tamaño de dicho archivo, de requerirse las pistas se restaurará la Copia de Seguridad.
h. Todos los cambios a programas deben realizarse en el ambiente de desarrollo, los desarrolladores no deben tener acceso a los ambientes de pruebas / Testing y producción.
i. Los desarrolladores deben tener acceso únicamente al ambiente de desarrollo y pruebas.

15.1.7. Ambientes de desarrollo.

a. Deben existir los mecanismos y herramientas necesarias que restrinjan el acceso a las bases de datos en las que se almacena la información institucional.
b. Debe existir una Base de Datos, con igual configuración y parametrización, por cada ambiente de trabajo.
c. Debe existir un Lenguaje de desarrollo, que garantice fácil integración con los demás sistemas de información de la entidad.

16. CONTROL DE LAS MODIFICACIONES

El manual y políticas de seguridad informática de Emprestur, se revisará y modificará según los requerimientos, permitiendo en esto la mejora continua del procedimiento y el control del documento bajo el cumplimiento de los requisitos legales aplicables a Emprestur y en la unidad de negocios o grupo empresarial.

El control de las modificaciones se dejará descritos en el FT-GEI-C-001 Listado Maestro y en la tabla Anexo control de modificaciones descrito a continuación.

ANEXO CONTROL A MODIFICACIONES

NÚMERO DE VERSIÓN	NUMERAL MODIFICADO	FECHA DE LA ELABORACIÓN O REVISIÓN	ELABORADO POR:	REVISADO POR:	APROBADO POR
01	Todo el documento	15/01/2017	Carlos Jaimes – Ingeniero Sistemas	Jose David Gallo - Director de Innovación y desarrollo	Andrea Mesa Montoya – Gerente General
02	Todo el documento	15/01/2024	Carlos Jaimes – Ingeniero Sistemas	Jose David Gallo - Director de Innovación y desarrollo	Andrea Mesa Montoya – Gerente General