Para dar cumplimiento a la política global de la seguridad de la información la organización ha establecido políticas anexas que deben ser divulgadas a la totalidad de los funcionarios de la compañía y los asociados de negocio.

INDICE DE POLITICAS

## ALCANCE

Las presentes políticas aplican a todas las dependencias y personal que componen la organización, y a la totalidad de procesos internos o externos, así como a terceros y en general a todos los asociados de negocio que tengan relación directa o indirecta con EASY LM.

## OBJETIVOS

- Proteger y administrar objetivamente la información de la compañía de la mano con las tecnologías utilizadas para este fin, evitando amenazas deliberadas o accidentales, asegurando el cumplimiento de las características de confidencialidad, integridad, legalidad, confiablidad y no rechazo de la información.
- Definición de directrices mediante las presentes políticas, para la correcta evaluación de los riesgos de seguridad de la información y su impacto.
- Establecer los diferentes parámetros para la protección de la organización frente a los diferentes riesgos que se pueden presentar.

## INCUMPLIMIENTO

El incumplimiento de cualquier política en general de la organización trae consecuencias negativas por pérdida de operatividad, retrabajo para restablecimiento de la información, posibles demandas, consecuencias legales y demás actividades que se puedan presentar, por ende el incumplimiento será sancionado según se establece las normas establecidas por la organización, sus acuerdos de seguridad, cláusulas contractuales con empleados y terceros, o de acuerdo el RIT (reglamento Interno de trabajo), y de acuerdo a lo estipulado en la normatividad del gobierno nacional en cuanto a seguridad y privacidad de la información se refiere.

## RESPONSABILIDADES

**Equipo de Seguridad de la Información:** Velar por el cumplimiento de la presente política, y apoyar en la definición de las directrices respecto a cómo tratar la información que se maneja en la organización tratando siempre de lograr el mejoramiento continuo.

**Personal:** Es responsabilidad del personal cumplir las directrices de la presente política, respetando las restricciones que se establezcan y haciendo buen uso de los derechos, permisos y privilegios que le hayan sido otorgados, pues cada usuario es responsable por sus acciones mientras usa cualquier recurso de Información.

**Asociados de negocio:** Todos los terceros vinculados a la cadena de suministro ya sean clientes, proveedores o terceros deberán cumplir las directrices de la presente política, respetando las restricciones que se establezcan y haciendo buen uso de los derechos, permisos y privilegios que le hayan sido otorgados mientras usa cualquier recurso de Información.

# POLÍTICA SEGURIDAD DE LA INFORMACIÓN

## GENERALIDADES

La política es de aplicación obligatoria para todo el personal de la compañía cualquiera que sea la situación contractual y el nivel de las tareas que desempeñe.

La gerencia de la compañía aprueba esta política y es responsable de la autorización de sus modificaciones.

El **comité de seguridad de la información** será el responsable de revisar y proponer recomendaciones, mejoras y estrategias de capacitación, así como el responsable de coordinar e impulsar la implementación y el cumplimiento de la política.

El **área de seguridad informática (Líder de IT)** será responsable de cumplir con funciones relativas a la seguridad de los sistemas de información de la compañía y el soporte a todas las áreas de la compañía relativo a este aspecto.

El **área de recursos humanos** notificara a todo el personal que se contrate las obligaciones respecto al cumplimiento de la política, procesos y procedimientos, será responsable de la notificación de la presente política y de los cambios que en ella se produzcan a todo el personal, deberá garantizar la firma de acuerdos de confidencialidad y de capacitar sobre los lineamientos establecidos.

## SEGURIDAD DE LA INFORMACIÓN EN EL RECURSO HUMANO

Todo el personal de la compañía sin importar su situación contractual o al departamento al que pertenecen, debe tener acceso a información de acuerdo con su perfil.

| CARGO | RESPONSABILIDAD | SUPERVISIÓN |
|---|---|---|
| **GERENTES** | Información de clientes, personal de la compañía, información financiera. | Líder del comité |
| **DISEÑADOR** | Información de clientes y proyectos. | Área y comité seguridad |
| **COORDINADOR NACIONAL** | Información de clientes y proyectos. | Área y comité seguridad |
| **COORDINADOR COMERCIAL** | Información de clientes y proyectos. | Área y comité seguridad |
| **ASISTENTE ADMITIVO** | Información de clientes y personal de la compañía. | Área y comité seguridad |
| **AGENTES CALL CENTER** | Información limitada de proyectos para la realización de sus funciones. | Área y comité seguridad |
| **AUDITORES** | Información limitada de proyectos para la realización de sus funciones. | Área y comité seguridad |
| **OPERARIOS** | Información limitada de proyectos para la realización de sus funciones. | Área y comité seguridad |
| **OFICIOS GENERALES** | NA | NA |
| **PROVEDORES** | Información limitada sobre el servicio específico que prestara para un proyecto determinado. | Área y comité seguridad |
| **CLIENTES** | Información general de la compañía y especifica del desarrollo del proyecto. | Área y comité seguridad |

**Nota:** Todo el personal externo debe estar autorizado por parte de la gerencia y el comité de seguridad de la información quienes serán responsables del control y vigilancia del uso adecuado de la información.

## SEGURIDAD FISICA

La protección física se llevará a cabo mediante la creación de medidas de control respecto a las instalaciones en oficinas generales y de las instalaciones de procesamiento de información.

Se protegerán especialmente las áreas que contienen instalaciones de procesamiento de información, energía eléctrica y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Se garantizará la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán medios alternativos de control de acceso físico al área o edificio. El acceso al edificio estará restringido exclusivamente al personal autorizado o visitantes controlados.

## SEGURIDAD EN LOS EQUIPOS

Los equipos que contengan información deben ser mantenidos en un lugar seguro y protegido por lo menos con:

- Contraseña para el inicio e ingreso del usuario al equipo
- Contraseña al entrar al correo o plataformas donde tenga acceso.
- Todo debe estar en la nube para evitar perdida de información en el equipo.
- Las actualizaciones de parches, códigos maliciosos y demás configuraciones del sistema deberán ser realizadas frecuentemente (al menos mensualmente) y deben ser ejecutadas por el líder de Seguridad.

### SUMINISTRO DE ENERGÍA

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla
en el suministro de energía.

2. Contar con un suministro de energía inin-terrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas.

### MANTENIMIENTO DE EQUIPOS

El área de seguridad realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

1. Someter el equipamiento a tareas de mantenimiento preventivo, físico al menos una vez al año y software de manera mensual.
2. Se mantendrá un listado o método de control del equipamiento con el detalle de la frecuencia en que se realiza el mantenimiento preventivo.
2. Se establece que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
3. se debe registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

**BAJA O REUTILIZACIÓN SEGURA DE LOS EQUIPOS**

La información puede verse comprometida por una baja o reutilización descuidada del equipamiento.

Los medios de almacenamiento que contienen material sensible serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

Todo equipo que vaya a ser reutilizado deberá ser formateado y se entregara seteado deacuerdo al perfil del nuevo usuario, siempre manteniendo un usuario administrador exclusivo del área de seguridad.

## POLÍTICA PARA DISPOSITIVO MÓVIL Y TELETRABAJO

### GENERALIDADES

Entre los equipos de computación móvil se incluyen todo tipo de ordenadores portátiles, teléfonos móviles, tarjetas de memoria y demás equipamiento móvil utilizado para almacenamiento, procesamiento y transferencia de datos.
El equipamiento mencionado precedentemente puede ser llevado fuera de las instalaciones solamente con autorización.

### Reglas básicas

Se debe tener especial cuidado cuando los equipos de computación móvil se encuentran en vehículos, espacios públicos, habitaciones de hotel, salas de reunión, centros de conferencias y demás áreas no protegidas exteriores a las instalaciones de la organización.

La persona que se lleva equipos de computación móvil fuera de las instalaciones debe cumplir las siguientes reglas:

- El equipamiento de computación móvil sea cual sea la clasificación de información que contenga no debe ser desatendido y, en lo posible, debe quedar resguardado bajo llave para asegurarlo.
- Cuando se utiliza equipamiento de computación móvil en lugares públicos, el usuario debe tener la precaución de que los datos no puedan ser leídos por personas no autorizadas.
- La conexión a redes de comunicación y el intercambio de datos debe reflejar la sensibilidad de los datos y se realiza de forma que no se comparte ninguna información del dispositivo móvil.
- Toda la información de datos personales y de negocio que se encuentra en ordenadores portátiles se debe cifrar.
- El líder de seguridad es el responsable de la capacitación y concienciación de las personas que utilizan equipamiento de computación móvil fuera de las instalaciones de la organización.
- Todo equipo debe ser protegido por la póliza de seguro empresarial.

### Teletrabajo

Tele-trabajo significa que los equipos de información y comunicación se utilizan para permitir que los empleados realicen su trabajo fuera de la organización. El tele-trabajo incluye el uso de teléfonos móviles fuera de las instalaciones de la organización.

El tele-trabajo debe ser autorizado por el líder de proceso a su equipo.

Se deben tener en cuenta las siguientes recomendaciones:

- Todo equipo debe moverse en una funda o maletín de protección que ofrezca buena resistencia a caídas, golpes o aplastamiento.
- Evitar el acceso no autorizado de personas que viven o trabajan en la ubicación donde se realiza la actividad de tele-trabajo. (no está autorizado el uso de equipos por personas ajenas a la organización)
- Configuración adecuada de la red local utilizada para conectarse a la Internet.
- Protección de los derechos de propiedad intelectual de la organización, tanto por el software como por otros contenidos que puedan estar protegidos por derechos de propiedad intelectual.
- Disponer de un espacio físico que le permita ejecutar las labores de trabajo cómodamente.
- Es recomendable usar un atril para apoyar el dispositivo y así evitar que caigan líquidos sobre él.
- Cableado en casa: Debe garantizarse un cableado ordenado que evite la caída del dispositivo.
- Siempre que el personal se ausente de su estación de trabajo deberá bloquear todos los equipos y dispositivos que de él dependen y/o utiliza.
- Una vez terminada la jornada laboral el equipo debe retirarse y guardarse en lugar seguro para evitar accesos o daños.
- Al activarse el protector de pantalla debe bloquear la sesión en los equipos de cómputo y dispositivos móviles, este deberá activarse después de 5 minutos de inactividad de cualquiera de estos equipos.

**Tablets y Smartphones**

Utilizar estos dispositivos para el entorno laboral implica también enviar y recibir correos electrónicos, atender llamadas de trabajo, almacenar información corporativa, tener acceso remoto a documentos en la nube, o incluso tener conversaciones por mensajería instantánea sobre temas laborales, por lo que son un elemento más a proteger.

- Se debe limitar el acceso al dispositivo mediante un bloqueo con contraseña, patrón o similar.
- Se debe disponer de medidas para poder localizar el dispositivo o hacer un borrado remoto del dispositivo en caso de pérdida o robo.
- Se debe instalar un antivirus para dispositivo móvil que pueda ser administrado.
- Se deben instalar siempre las últimas actualizaciones de seguridad de los programas y sistemas operativos.

# POLÍTICA DE CONTROL DE ACCESO

## GENERALIDADES

Controlar quien accede a la información de la compañía es un primer paso para protegerla. Es esencial que podamos decidir quién tiene permisos para acceder a nuestra información, como, cuando y con qué finalidad.

A continuación, se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo al control de acceso.

Las políticas establecidas por la organización para la protección de la información, asigna los permisos necesarios para que cada usuario o grupo de usuarios solo puedan realizar las acciones necesarias sobre la información a la que tienen acceso.

## REGLAS BASICAS

### Registro de Usuarios.

1. Para la creación/modificación/borrado de cuentas de usuario y permisos de acceso se define y aplica el formato DG-FO001, esta solicitud será hecha por vía email, con la finalidad de dejar la trazabilidad de los usuarios y cuentas procesadas.
2. Se deben gestionar las cuentas de administración de sistemas y aplicaciones teniendo en cuenta su criticidad y el cargo.
3. Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
4. Verificar que el usuario tiene autorización del propietario de la Información para el uso del sistema, base de datos o servicio de información.
5. Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad.
6. Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.
7. Mantener un registro formal de todas las personas registradas para utilizar el servicio.
8. Al finalizar la relación contractual con el empleado, es necesario revocar sus permisos de accesos a nuestros sistemas e instalaciones. Se bloquearán sus cuentas de correo, sus cuentas de acceso a los repositorios, servicios y aplicaciones. Además, exigiremos la devolución de cualquier activo de información que se le hubiese asignado (tarjetas de acceso o de crédito, equipos, dispositivos de almacenamiento, tokens criptográficos, etc.).
9. Efectuar revisiones periódicas con el objeto de:
    - Cancelar identificadores y cuentas de usuario redundantes.
    - Inhabilitar cuentas inactivas por más de 30 días.
    - Eliminar cuentas inactivas por más de 60 días, previa consulta a líder de área.

**Administración de Privilegios.**

1. Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad Informática.
2. Los sistemas multiusuario que requieren protección contra accesos no autorizados deben prever una asignación de privilegios controlada:
   - Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.
   - Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.
   - Mantener un proceso de autorización y un registro de todos los privilegios asignados.
   - Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

**Administración de Contraseñas de Usuario**

La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

1. Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificando el usuario.
2. Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña.
3. Almacenar las contraseñas sólo en sistemas informáticos protegidos.
4. Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo, verificación de huellas dactilares), doble factor de autenticación, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc.

**Control de Acceso a la Red**

1. Las conexiones no seguras a los servicios de red pueden afectar a toda la infraestructura, por lo tanto, el responsable del área de seguridad controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de los mismos.

2. El responsable del Área de seguridad tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido de un líder de área que lo solicite.
3. Creación de red WIFI para invitados con limitaciones de uso y control desde el Access point y firewall.
4. Identificar las redes y servicios de red a los cuales se permite el acceso.
5. Establecer controles para proteger el acceso a las conexiones y servicios de red.

**Control de Acceso a internet**

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

1. Se tendrá acceso restringido a internet a ciertos grupos de páginas bloqueados por default desde el antivirus y firewall.
2. Solo los usuarios elevados podrán tener acceso sin restricción a paginas seguras debido a las necesidades de negocio.
3. Toda pagina no segura debe ser bloqueada por firewall y antivirus.
4. Se generarán registros a través del firewall y el antivirus de los accesos a internet de los usuarios, con el objeto de realizar revisiones o analizar casos particulares de situaciones que pongan en riesgo la seguridad de información.

**Control de Acceso al Sistema Operativo.**

1. El Responsable de Seguridad Informática garantizara que el acceso al sistema operativo de los equipos de cómputo este restringido a través de la administración de políticas desde el directorio activo.
2. Cada computador corporativo deberá tener una cuenta de administrador que será manejada por el líder de seguridad y una cuenta atada al directorio activo del usuario final del equipo.

**Cuentas de administración.**

Las cuentas de administración permiten realizar cualquier acción sobre los sistemas que administran, por lo que deben ser gestionadas con la máxima precaución. Tendremos en cuenta los siguientes aspectos:

1. Utilizar este tipo de cuentas únicamente para realizar labores que requieran permisos de administración.
2. Evitar que los privilegios de las cuentas de administrador puedan ser heredados.
3. Las claves de acceso deben ser lo más robustas posibles y ser cambiadas con frecuencia.

**Grupos de acceso**

Los accesos se concederán dependiendo del perfil definido anteriormente, definiremos también una serie de grupos que tendrán determinados accesos para cada tipo de plataforma así:

| GRUPO | MICROSOFT | KIZEO | EASY FIEL | BANCOS | ONE DRIVE | ENTIDADES ESTADO Y PRIVADAS | PORTALES CLIENTES | ANTIVIRUS | FIREWALL | DIRECTORIO ACTIVO |
|---|---|---|---|---|---|---|---|---|---|---|
| GERENCIA | 365 PREMIUM | ADMINISTRADOR | LIDER AREA | APROBADOR | CONTROL TOTAL | CORPORATIVO POR ENTIDAD | CORPORATIVO POR CLIENTE | NO APLICA | NO APLICA | NO APLICA |
| ASIST COM Y FIN | 365 PREMIUM | NO APLICA | NO APLICA | PREVALIDADOR | EDICION | CORPORATIVO POR ENTIDAD | CORPORATIVO POR CLIENTE | NO APLICA | NO APLICA | NO APLICA |
| DISEÑO | 365 ESTANDAR | NO APLICA | NO APLICA | NO APLICA | EDICION | NO APLICA | NO APLICA | NO APLICA | NO APLICA | NO APLICA |
| EJECUCION | 365 ESTANDAR | LIDER DE EQUIPO | COORDINADOR | NO APLICA | EDICION | NO APLICA | NO APLICA | NO APLICA | NO APLICA | NO APLICA |
| OPERATIVO | 365 BASICO | USUARIOS | AGENTE | NO APLICA | NO APLICA | NO APLICA | NO APLICA | NO APLICA | NO APLICA | NO APLICA |
| SEGURIDAD | 365 BASICO | NO APLICA | NO APLICA | NO APLICA | NO APLICA | NO APLICA | NO APLICA | ADMINISTRADOR | ADMINISTRADOR | ADMINISTRADOR |

GRUPOS ACCESO.xlsx

Asignación de permisos. Una vez establecidos los tipos de información, los perfiles de usuarios y los grupos existentes, podremos concretar los tipos de acceso a la información a los que tienen derecho. Los permisos

concretarán que acciones pueden realizar sobre la información (creación, lectura, borrado, modificación, copia, ejecución, etc.). Como norma general siempre se otorgará el mínimo privilegio en el establecimiento de los permisos.

## POLÍTICA SOBRE EL USO DE CONTROLES CRIPTO GRÁFICOS

### GENERALIDADES

Con el fin de garantizar la confidencialidad e integridad de algunos documentos designados como sensibles, la entidad debe utilizar sistemas y técnicas criptográficas para la protección de la información. El sistema de información debe implementar mecanismos de protección de información que cumplan con la reglamentación, políticas, estándares, guías aplicables, así como:

- Proporcionar una protección adecuada a los equipos utilizado para generar, almacenar y archivar claves, considerándolo crítico o de alto riesgo.
- Proteger las claves secretas y privadas evitando sean copiadas o modificadas sin autorización.

La organización deberá velar porque la información de su custodia o propiedad que es catalogada como publica reservada o pública clasificada se cifre al momento de almacenarse o transmitirse por cualquier medio. Para dar cumplimiento al tratamiento definido para los activos de información, todos los involucrados en el alcance deben cumplir, las siguientes directrices:

**Directrices de seguridad para todo el personal:**

- La información que contenga contraseñas de usuario o claves para el control de acceso a los sistemas de información no podrá ser almacenada en texto plano y deberá hacer uso de mecanismos criptográficos.
- Todos los documentos que se han cifrado y descifrado, en caso que se requiera, deberán ser almacenados y tratados con las medidas de seguridad requeridas conforme al grado de clasificación de la información.
- Se deberá identificar todo sistema de información que requiera realizar transmisión de información pública reservada y pública clasificada, para así garantizar que cuente con mecanismos de cifrado de datos.
- Se deberán cifrar los discos duros de los equipos de cómputo que contengan información pública reservada o pública clasificada.
- El manejo de llaves criptográficas se debe realizar de acuerdo con los lineamientos establecidos en la **Política de Gestión de Llaves Criptográficas**.

**Directrices de seguridad para el personal encargado de la configuración**

Deberá configurar y administrar el sistema de cifrado, así como velar por el cumplimiento de la presente política y generar los reportes que se requieran.

# POLÍTICA GESTIÓN DE LLAVES CRIPTOGRÁFICAS

## GENERALIDADES

La organización vela porque la información que custodie o de la cual sea propietaria, y que se encuentre catalogada como pública clasificada o pública reservada, sea cifrada al momento de almacenarse y transmitirse por cualquier medio.
El área de seguridad será la persona responsable y encargada de la activación, recepción y la distribución de las llaves criptográficas a los usuarios autorizados y velará porque la llave se encuentre activa en el periodo de tiempo previsto.

Los responsables de las llaves criptográficas deberán almacenar las llaves de forma segura y se comprometerán a restringir el acceso sólo a los usuarios autorizados. De igual forma, una copia de las llaves (si esta existe) deberá ser almacenada en sitio seguro para su recuperación en caso tal que esta se extravíe.

El cambio o actualización de las llaves deberá ser solicitado por el líder de área, cada 6 meses ejecutado por el área de seguridad o cuando salga alguien de la organización con manejo de información bajo llaves.

Las llaves serán revocadas por el área de seguridad o persona delegada, cuando exista sospecha de que pudieron ser accedidas por una persona no autorizada o cuando un colaborador culmine su relación con la organización.

Para todas y cada una de las actividades pertenecientes a la administración, gestión y eliminación de las llaves criptográficas, se deberá mantener registro de las actividades realizadas.

Los sistemas que actualmente cuenten con algún mecanismo de cifrado deben acogerse a la presente política.

# POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIA

## GENERALIDADES

Se debe adoptar por parte de Easy LM SAS una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles, equipos de cómputo a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información.

### Ubicación de Escritorios y Equipos

Los sitios de trabajo del personal de la compañía deben localizarse en ubicaciones donde este limitado el acceso de personas externas, todo dentro de oficinas o lugares que puedan ser cerradas bajo llave, especialmente las posiciones que tienen acceso a información confidencial.

### Escritorios limpios

1. Siempre que el personal se ausente de su estación de trabajo, deberá guardar en un lugar seguro y bajo llave cualquier documento físico, medio magnético u óptico que contenga información pública de uso interno, restringida o confidencial.
2. Al finalizar la jornada de trabajo, los colaboradores deberán guardar en un lugar seguro los documentos y medios que contengan información pública de uso interno, restringida o confidencial, además bloquear los equipos de cómputo (por ejemplo, bloquear los equipos con sistema operativo Windows con las teclas Windows + L y no solo apagar el monitor).
3. Siempre que imprima información pública de uso interno, restringida o confidencial se deberá retirar inmediatamente de las impresoras.
4. Todo documento impreso que contenga información confidencial y que ya no se requiera para su uso deberá ser destruido en la picadora.
5. Todo computador deberá estar protegido por guaya o guardado en cajón bajo llave para evitar su perdida.

### Pantallas limpias

- La pantalla de computador (escritorio) debe estar libre de archivos o enlaces de acceso a archivos, estos deben ubicarse en las debidas carpetas de almacenamiento en la nube.
- Siempre que el personal se ausente de su estación de trabajo, deberá bloquear las sesiones de sus equipos de cómputo.
- Todos los equipos de cómputo y dispositivos portátiles deberán tener aplicado el cierre de sesión por inactividad, definido por el equipo de seguridad de la información.
- Siempre que el personal se ausente de su estación de trabajo deberá bloquear todos los equipos y dispositivos que de él dependen y/o utiliza.
- Al activarse el protector de pantalla debe bloquear la sesión en los equipos de cómputo y dispositivos móviles, este deberá activarse después de 5 minutos de inactividad de cualquiera de estos equipos.

### Equipos de reproducción de información

Los equipos de reproducción de información (impresoras, fotocopiadoras, escáneres, etc.), deben estar ubicados en lugares de acceso controlado y cualquier documentación con información pública de uso interno, restringida o confidencial. se debe retirar inmediatamente del equipo y ser puesta en un lugar seguro.

# POLÍTICA DE RESPALDO DE LA INFORMACIÓN

## GENERALIDADES

La organización dispone de la nube con el fin de que los usuarios hagan uso de esta, con el objetivo de mantener la información disponible y actualizada, en esta se debe subir y mantener la información con los accesos y seguridad necesaria de acuerdo al tipo de información

Toda información que se encuentre en la nube permanecerá en los servidores y será de fácil recuperación en momento de alguna perdida, el proveedor tiene el servicio de mirroring para todas las cuentas corporativas, por este motivo no se hacen copias de seguridad y los usuarios tienen la responsabilidad de hacer un buen uso de la nube y subir la información pertinente a esta.

Toda la información será almacenada en la nube y se trabajará directamente en ella desde herramientas de escritorio o web, ninguna información de negocio será almacenada de manera local en el disco duro del computador el cual no tiene respaldo.

Las carpetas disponibles en la nube serán entregadas como activo de información y se le dará acceso a cada empleado dependiendo de las necesidades de negocio y de su rol, se deberá hacer una revisión al menos cada seis meses o cada vez que un empleado termine su contrato con la compañía para ajustar lo necesario.

## PLATAFORMAS DE TRABAJO UNICAS APROBADAS

Los contratos de servicios con plataformas digitales, software etc pueden cambiar en el tiempo debido a la aparición de nuevos competidores o la mejora de servicios, seguridad, precios etc, EASY LM ha escogido las siguientes para poder administrar su operación:

MICROSOFT 365

- OUTLOOK: Correo corporativo
- ONE DRIVE: Almacenamiento en la nube
- SHAREPOINT: Intranet corporativo
- PLANNER: Seguimiento y productividad
- TEAMS: Reuniones, grupos, compartir data

EASY FIEL: Plataforma desarrollo in house.
KIZEO FORMS: Documentación de procesos
WOLKVOX: Call center
EFECTY: Giros nacionales
LANUZA SOFT: Soporte a equipos.
AZURE: Servicio de en la nube para implementación de aplicaciones.

# POLÍTICA Y PROCEDIMIENTOS DE TRANSFERENCIA DE INFORMACIÓN

## GENERALIDADES

Para el cumplimiento de sus obligaciones EASY LM intercambia de información con diferentes entes y por diferentes medios, por ello es necesario establecer unos lineamientos que garanticen que el intercambio de dicha información se realiza bajo los niveles de protección adecuados siempre que se vaya a transferir información ya sea personal, información pública clasificada o pública reservada, quien está enviando la información deberá confirmar que **cuenta con la autorización expresa del titular del dato o su representante para su tratamiento**.

### Intercambio de Información entre empleados

Solo se puede realizar intercambio de información entre el personal activo y cuando dicho intercambio corresponda a actividades relacionadas con el desarrollo de sus labores.

Siempre que se realice intercambio de información catalogada como pública clasificada o pública reservada, dicho intercambio debe ser aprobado por el jefe inmediato.

### Intercambio de información con terceros.

Todo intercambio de información electrónica con terceros debe ser respaldado con un acuerdo de confidencialidad y no divulgación de la información proporcionada.

La solicitud de intercambio de información puede ser por requerimientos internos, de un organismo externo o incluso de un tercero que, ante disposiciones legales o directrices del gobierno hacen necesaria dicha interoperabilidad.

La información recibida de otra entidad en Colombia se debe salvaguardar de acuerdo con la política de seguridad de información de Easy LM

El intercambio de información digital pública clasificada y pública reservada, debe realizarse por canales cifrados que garanticen la protección de la confidencialidad de la información y que cumpla con la política de controles criptográficos.

### Intercambio de Información Física

Easy LM no manejara información física toda la información será digitalizada y almacenada de manera organizada ya sea interna o de clientes.

### Intercambio de información vía correo electrónico institucional

Toda información enviada desde Easy LM a través de correos electrónicos deberá incluir en su pie de página la siguiente advertencia:

Este mensaje y cualquier archivo que se adjunte al mismo es confidencial y contiene información clasificada y reservada de Easy LM SAS, para el uso exclusivo de su destinatario. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje es prohibida y sancionada por la ley. Si

por error recibe este mensaje, por favor reenviarlo al remitente y borrar el mensaje recibido inmediatamente.

## POLÍTICA DE DESARROLLO SEGURO

### GENERALIDADES

EASY LM no es una organización dedicada al desarrollo de software por tanto sus desarrollos son manejados externamente, la presente política vela porque el desarrollo de los sistemas de información cumpla con los requerimientos de seguridad definidos basado en buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad.

Se asegura que todo software desarrollado o adquirido, cuenta con el nivel de soporte requerido.

### Separación de entornos

Toda aplicación deberá estar desarrollada con los siguientes ambientes:

1. Ambiente Desarrollo (Proveedor)
2. Ambiente Producción (Easy LM)
3. Ambiente Producción secundario (Easy LM) Este dependerá si el cliente decide pagar doble soporte.
4. Ambiente Testing (Easy LM)

Los ambientes de desarrollo, prueba y producción estarán separados preferentemente en forma física por tanto se ubicarán en servidores en diferentes localizaciones.

### Análisis de Vulnerabilidades

El equipo de desarrollo deberá efectuar análisis de vulnerabilidades ya sea usando servicios con herramientas digitales o mediante la contratación de ethical hacking a proveedores especializados, esto deberá documentarse y manejarse deacuerdo a procedimientos y se ejecutara cada vez que salga una nueva aplicación, que se haga un nuevo reléase o mensualmente. (ethical Hacking anual)

### Análisis de Código

El equipo de desarrollo deberá efectuar análisis de código fuente a través del uso de herramientas digitales (Ejem: Resharper, Lint), esto deberá documentarse y manejarse deacuerdo a procedimientos y se ejecutará cada vez que salga una nueva aplicación, que se haga un nuevo reléase o mensualmente.

### Cuentas de acceso

Todas las aplicaciones deben estar implementadas en servicios en la nube contratados directamente por Easy LM, se creará una cuenta de administración con acceso elevado para administrar facturación y accesos a equipos de desarrollo.

**Gestion de Hallazgos**

Todos los hallazgos se manejarán deacuerdo a su nivel de riesgo, Critico y Alto deberán ser corregidos de inmediato, para riesgo medio y bajo será considerado junto con el equipo de seguridad para manejo en corto plazo.

**Gestion de LOGs**

Se determinarán cuales son los LOG más estratégicos para hacer seguimiento al sistema, muchas plataformas en la nube ya tienen servicios de LOG Analysis incluido, se debe entonces habilitar el servicio para tener disponibilidad de data.
La data se debe descargar al menos una vez por mes y desagrear en un reporte para evidenciar tendencias o hallazgos.
Se deben configurar alertas para LOGs críticos que avisen de manera temprana a los administradores del sistema de cualquier irregularidad.

**Multifactor de autenticacion**

Todo acceso de usuarios al back end debe tener multifactor de autenticación preferiblemente a través de correo electrónico o SMS.

**Ataques de Fuerza bruta**

Implementar un control para evitar este tipo de ataques y que garantice que el acceso no sea de un robot. Ej captcha, bloqueo por retardo en el número de intentos fallidos, etc.

**Contraseñas seguras**

Garantizar que al hacer el cambio de contraseña se ingrese la contraseña actual.
El token debe ser generado con mínimo 6 caracteres de longitud.
Establecer una política para la creación de contraseñas seguras.

**Ofuscación**

Ofuscar de manera segura el código fuente antes de liberar el apk a producción.

**Cierre de sesión**

Cerrar las sesiones cuando permanezcan inactivas más de 5 minutos.
Las cookies de sesión deben caducar cuando se cierra una sesión.

**Cifrado de información**

Desplegar la aplicación sobre un canal de comunicación cifrado, como, por ejemplo: HTTPS utilizando TLS.
Encriptar toda información sensible en tránsito.

Cifrar o hashear todas las credenciales de autenticacion almacenadas.
Utilizar solo algoritmos de cifrado estandarizados y ampliamente revisados.

**Firewall**

Activar el servicio de firewall y ejecutar pruebas de seteo hasta hallar el modelo adecuado que brinde un balance entre capacidad de uso y seguridad.
Crear reglas de denegación por omisión que se despliegan a todo el tráfico excepto aquellos servicios y puertos que se hayan permitido explícitamente.

**Desarrollador**

Todo desarrollador debe certificar que tiene entrenamiento en escritura de código seguro para su especifico medio y responsabilidades de desarrollo.

**Gestión de incidentes**

Todo incidente debe ser documentado y procesado deacuerdo al formato hasta lograr un cierre adecuado, los incidentes tendrán una clasificación de riesgo lo cual permitirá entender que tan rápido deben ser abordados y solucionados.

**Autorización de tratamiento de datos y términos y condiciones de uso**

Todo sistema de información que capture información personal debe incorporar un mecanismo de autorización de tratamiento de datos personales y una aceptación de términos y condiciones de uso de la aplicacion.

**Autorización Política de cookies**

Todo sistema de información creado ya sea web o apps debe reflejar y solicitar autorización de la política de cookies.

**Software actualizado**

Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión estable publicada por el fabricante.
Asegurar que las aplicaciones y desarrollos se diseñen y construyan en versiones vigentes y estables emitidas por el fabricante respecto a las herramientas, componentes, lenguajes de programación.

**Acuerdo de licenciamiento**

Asegurar que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

**Validación de datos**

Construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de

los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

## POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON PROVEEDORES

### GENERALIDADES

Requisitos de seguridad en productos y servicios. Debemos definir los requisitos en Ciberseguridad que deben cumplir los productos o servicios que adquirimos a proveedores. Estos requisitos serán coherentes con las políticas de seguridad de la información de la organización y los extenderemos a proveedores, suministradores, colaboradores, partners, canales de ventas y distribución, etc.

Definir cláusulas contractuales en materia de seguridad de la información con el fin de establecer contratos o acuerdos rigurosos en materia de ciberseguridad, debemos detallar las cuestiones más relevantes que deben reflejarse en los contratos con nuestros proveedores.

Determinar qué información es accedida, cómo puede ser accedida y la clasificación y protección de esta.

Asegurarnos que una vez finalizado el contrato, el proveedor ya no podrá acceder o mantener la información sensible de nuestra organización; reflejar los requisitos legales oportunos:

- Cumplimento de los derechos de propiedad intelectual.
- Reflejar el derecho de auditoría y de control sobre aspectos relevantes del acuerdo
- Incluir las situaciones que conlleven la finalización del contrato
- Definir las garantías específicas
- Penalizaciones económicas en caso de incumplimiento
- Perjuicios económicos por inactividad.
- Certificaciones y garantías adicionales.

**Controles de seguridad obligatorios.** Para asegurar la contratación de un servicio externo seguro debemos identificar los controles de seguridad que consideramos de obligado cumplimiento. Estos controles deben tener en cuenta los siguientes aspectos:

- Servicios y componentes informáticos a los que la organización permite el acceso.
- Qué información relevante de la organización puede ser accedida y con qué método de acceso.
- Como gestionar cualquier incidencia relacionada con el acceso de los proveedores a nuestros sistemas.

**Formar parte de los foros y organizaciones de usuarios de los productos/servicios software utilizados.** Puede resultar de gran interés participar en foros y asociaciones sobre productos que hayamos adquirido. De esta manera tendremos la posibilidad de consultar las principales funcionalidades, novedades y vulnerabilidades acerca de los mismos. Además, revisaremos la reputación de nuestros proveedores, así como las certificaciones y sellos de calidad que poseen.

**Certificación de los servicios contratados**. En servicios especialmente críticos podemos exigir a las empresas la garantía de que posean algunas de las certificaciones referentes a la calidad en la gestión de la seguridad de la información.

**Auditoría y control de los servicios contratados**. Para asegurar en todo momento la calidad del servicio contratado debemos establecer la manera de monitorear, revisar y auditar el servicio de tus proveedores en aspectos relacionados con la ciberseguridad. Necesitaremos establecer la manera de gestionar cualquier problema surgido con productos o servicios de nuestros proveedores.

**Finalización de la relación contractual.** Es importante garantizar la seguridad de la información tras la finalización de los servicios contratados. Para ello debemos formalizar las acciones a llevar a cabo una vez finalizado el servicio:

- Señalar los activos que han de ser devueltos
- Eliminación de permisos de acceso
- Borrado de información sensible de la organización almacenada en los sistemas del proveedor.