

	POLITICA		PAGINA	1 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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

- Política seguridad de la Información-----03
- Política para dispositivo móviles y teletrabajo-----05
- Política de control de acceso-----07
- Política sobre el uso de controles criptográficos -----09
- Política gestión de llaves criptográficas-----10
- Política de escritorio y pantalla limpia -----11
- Política de respaldo de la información-----13
- Política y procedimientos de transferencia de información-----14
- Política de desarrollo seguro-----15
- Política de seguridad de la información para las relaciones con proveedores----17
- Política de uso aceptable de activos-----19

	POLITICA		PAGINA	2 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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, confiabilidad 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.

	POLITICA		PAGINA	3 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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 seguridad)** 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
LIDERES DE EJECUCION	Información limitada de proyectos para la realización de sus funciones.	Área y comité seguridad
OFICIOS GENERALES	Cualquier información impresa que deba ser pasada por la picadora de papel	Asist administrativa y comité seguridad
PROVEDORES	Información limitada sobre el servicio específico que prestara para un proyecto determinado.	Área y comité seguridad
CLIENTES	Información general de la compañía y específica 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.

	POLITICA		PAGINA	4 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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 electrónico al área o edificio. El acceso al edificio estará restringido exclusivamente al personal autorizado.

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:

1. 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 back up (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 trimestral.
2. Se mantendrá un listado o método de control del equipamiento con el detalle de la frecuencia en que se realiza el mantenimiento preventivo.
3. Se establece que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
4. se debe registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

	POLITICA		PAGINA	5 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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.
- El antivirus será el mecanismo de protección para la conexión en lugares distintos a las oficinas generales.
- No esta permitido la conexión en redes abiertas (Sin clave de acceso)
- 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.
- En caso de daño o perdida el usuario responsable del equipo debe reportarlo de forma inmediata al departamento de seguridad para el respectivo bloqueo de accesos evitando asi la fuga de información.

	POLITICA		PAGINA	6 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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 área 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).
- Los equipos de cómputo deberán moverse en vehículos propios del empleado, líder de área o usando un servicio de Uber, taxi o similar, el uso del servicio de bus urbano/ nacional no esta permitido para el transporte de equipos.
- 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.

	POLITICA		PAGINA	7 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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 garantizar 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

1. Para la creación/modificación/borrado de cuentas de usuario y permisos de acceso se define y aplica el formato SG-DO015, y la aplicación de procedimientos:
 - SG-PD008 PROCEDIMIENTO ASIGNACION ACCESO
 - SG-PD011 PROCEDIMIENTO REVOCACION DE ACCESOS
2. Todas las cuentas de acceso a herramientas digitales serán procesadas con la misma rapidez y diligencia.
3. El identificador único de usuarios será la dirección de correo electrónico, para todas las plataformas corporativas, la idea es que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.
4. Los gestores (Líder seguridad – Coordinadores) de acceso siempre deben tener claro cuál es el perfil de la persona que va a ingresar, las necesidades de acceso y restricciones están descritas en el siguiente documento.
 - SG-DO004 LISTADO DE SOFTWARE Y ACCESOS
5. Aun cuando existe un lineamiento los gestores de acceso deben 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 trimestrales con el objeto de:
 - Cancelar identificadores y cuentas de usuario redundantes.
 - Verificar número de usuarios, perfiles y accesos otorgados.
 - Eliminar cuentas inactivas.

	POLITICA	PAGINA	8 de 1
	ANEXOS POLITICA GLOBAL	CA-PO015	
		VERSION	1

Administración de Privilegios.

- Los Gerentes de área serán los encargados de actualizar el documento de acceso, lo cual será supervisado por el Líder de Seguridad Informática.

SG-DO004 LISTADO DE SOFTWARE Y ACCESOS

- Como base para la elección de privilegios por perfil se tendrá en cuenta:
 - Identificar los privilegios asociados a cada producto del sistema.
 - Asignar los privilegios a individuos sobre la base de la necesidad de uso.
 - Analizar los riesgos de acceso de cada autorización otorgada.

Administración de Contraseñas de Usuario

La asignación de contraseñas se manejará de acuerdo a las características de cada plataforma así:

Microsoft 365

- Líder de seguridad entregara la contraseña provisional (previa solicitud creación de usuario).
- Una vez se efectuó el primer LOG IN, el sistema solicitara cambio de contraseña.
- El líder de seguridad activara el segundo factor de autenticación con el uso de Microsoft authenticator como opción principal.
- El sistema solicitara cambio de contraseña cada 3 meses.

Kizeo

- El coordinador una vez haya creado el usuario previa solicitud, generara a través del sistema una solicitud automática (Via Mail) al nuevo usuario para la creación de contraseña.
- El nuevo usuario generará su propia contraseña de acuerdo a la política del tercero (8 caracteres, y debe contener al menos una letra y un número).

Easy fiel

- Coordinador entregara la contraseña provisional (previa solicitud creación de usuario).
- Una vez se efectuó el primer LOG IN, el usuario deberá cambiar su contraseña.
- Se activará automáticamente el segundo factor de autenticación a través de un código por correo.

Plataformas especiales

Bancos: Se utilizarán 2 tipos de usuario:

- Prevalidador: Usado por la asistente administrativa para el posteo de transacciones.
- Aprobador: Usado por el líder de área financiera para la aprobación de transacciones posteadas.

Plataformas con aliados negocio

Los aliados de negocio se refieren a entidades con las que la empresa tiene relación tales como: EPS , ARL, aseguradoras, pago de aportes seguridad social , medicina prepagada , portales proveedores , clientes etc etc , estos usuarios y contraseñas serán manejados en una carpeta administrativa y un archivo excel encriptado.

	POLITICA		PAGINA	9 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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 proceso de seguridad tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo con el pedido de un gerente 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 de negocio,

1. se tendrá acceso restringido a internet a ciertos grupos de páginas bloqueados por default desde el antivirus y firewall.
2. Se creará algunas categorías de usuarios dentro de las plataformas con el objetivo de configurar más fácilmente los grupos de uso y se aseguraran los bloqueos utilizando como referencia el siguiente documento:

SG-DO004 LISTADO PERFILES ACCESOS Y RESTR

3. Toda página 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.

Perfiles de acceso

	POLITICA		PAGINA	10 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

Una vez establecidos los tipos de información y los perfiles de usuarios 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 necesario en el establecimiento de los permisos.

Los accesos se concederán dependiendo del perfil definido por las gerencias de área y se guiara por el siguiente documento:

SG-DO004 LISTADO DE SOFTWARE Y ACCESOS

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:

Publica
Confidencial
 interna

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.

	POLITICA		PAGINA	11 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

- 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 **2 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.

	POLITICA	PAGINA	12 de 1
	ANEXOS POLITICA GLOBAL	CA-PO015	
		VERSION	1

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, 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.

Escritorio físico limpio

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 restringida o confidencial.
2. El escritorio deberá estar libre de documentos y de tener impresiones deberán manejarse en la bandeja organizadora, ninguno de los documentos impresos debe ser de carácter confidencial o restringido.
3. Al finalizar la jornada de trabajo, los colaboradores deberán guardar en un lugar seguro los documentos y medios que contengan información 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).
4. Siempre que imprima información confidencial o interna se deberá retirar inmediatamente de las impresoras.
5. Todo documento impreso que contenga información confidencial y que ya no se requiera para su uso deberá ser destruido en la picadora.
6. Todo computador deberá estar protegido por guaya o guardado en cajón bajo llave para evitar su pérdida.

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.
- Solo se permitirá el uso de una carpeta para manejo de archivos temporales en escritorio (Descargas recientes, cálculos rápidos, etc.) esta no deberá contener información confidencial.
- 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.
- Todos los equipos de cómputo y dispositivos portátiles deberán tener aplicado el cierre de sesión por inactividad, este deberá activarse después de 2 minutos de inactividad y será seteado por el equipo de seguridad de la información.

	POLITICA	PAGINA	13 de 1
	ANEXOS POLITICA GLOBAL	CA-PO015	
		VERSION	1

Accesos directos en escritorio

Por default se setearan accesos directos a papelera de reciclaje, descargas, one drive y any desk.

Equipos de reproducción de información

Los equipos de reproducción de información (impresoras, fotocopadoras, escáneres, etc.), deben estar ubicados en lugares de acceso controlado y cualquier documentación con información de uso restringido 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 un servicio de almacenamiento en 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 con el tipo de información.

Toda información que se encuentre en la nube permanecerá en los servidores del proveedor microsoft y será de fácil recuperación en momento de algún incidente, microsoft tiene el servicio de mirroring para todas las cuentas corporativas haciendo copias de seguridad diarias con vigencia hasta 30 días, 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 tres 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

EFACTY: Giros nacionales

	POLITICA		PAGINA	14 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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 maneja 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

	POLITICA		PAGINA	15 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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 de acuerdo a procedimientos y se ejecutará 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 de acuerdo 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.

	POLITICA		PAGINA	16 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

Gestion de Hallazgos

Todos los hallazgos se manejarán de acuerdo 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 desagregar 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.

	POLITICA		PAGINA	17 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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 específico medio y responsabilidades de desarrollo.

Gestión de incidentes

Todo incidente debe ser documentado y procesado de acuerdo 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 aplicación.

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.

	POLITICA	PAGINA	18 de 1
	ANEXOS POLITICA GLOBAL	CA-PO015	
		VERSION	1

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, partes, 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:

- Cumplimiento 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.

	POLITICA		PAGINA	19 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

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.

POLÍTICA USO ACEPTABLE DE ACTIVOS

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

Definir las pautas para realizar un uso seguro y aceptable de los activos de información.

1. Responsabilidad de los activos

Todos los activos de la información tendrán un propietario designado en el inventario de activos. El propietario del activo será responsable de la confidencialidad, integridad y disponibilidad de la información del activo.

2. Retiro de los activos físicos

Los activos físicos podrán ser retirados de su lugar de almacenamiento o uso, siempre y cuando el responsable realice la solicitud y sea correctamente identificado. La solicitud de retiro de activos físicos deberá ser realizada por el líder de área responsable, formalizando la petición vía correo electrónico.

3. Devolución de los activos

Ante la desvinculación de trabajo, todos los activos y dispositivos de información deberán ser devueltos por el colaborador y se generara un documento de paz y salvo.

	POLITICA		PAGINA	20 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

4. Respaldo de la información

Toda información de negocio será almacenada en las carpetas compartidas designadas a cada area en la nube, ninguna información debe ser almacenada de manera local en el disco duro de los equipos de cómputo, se efectuará una copia periódica la cual será almacenada en una nube alterna de un proveedor autorizado.

5. Monitoreo del uso de los sistemas de información y comunicación

Todos los datos creados, almacenados, enviados o recibidos a través de los sistemas de información, u otros sistemas de comunicación de la organización (incluidas las aplicaciones, correos electrónicos, entre otros) se consideran propiedad de Easy LM SAS, por lo que la organización se reserva el derecho de monitorear y acceder al contenido de todas y cada una de las comunicaciones electrónicas y telefónicas de un usuario.

6. Instalación del software

La instalación de cualquier software no aprobado (software no reconocido como parte de los sistemas necesarios para el negocio) estará estrictamente prohibida en los equipos que son de propiedad de la compañía. cualquier software que requiera instalarse temporalmente a pedido del servicio deberá solicitarse al líder de área y al líder de seguridad.

7. Responsabilidad de las cuentas de usuario

El usuario no deberá, directa o indirectamente, permitir que otros utilicen sus derechos acceso. Es decir, no deberá usar el nombre de usuario y/o contraseña de otra persona.

8. Acceso a Internet

- Cualquier información que se acceda, transmita, reciba o produzca en internet está sujeta a divulgación y auditoría.
- Los equipos, la tecnología y los servicios provistos para el acceso a internet son propiedad de Easy LM, que puede analizar y si es necesario, bloquear cualquier archivo, sitio web, correo electrónico, dominio o aplicación almacenadas en la red internet o en las áreas privadas de la red, para garantizar el cumplimiento de la política de la seguridad de la información.
- Cualquier intento de cambiar los parámetros de seguridad por parte de cualquier empleado sin la debida acreditación y autorización para hacerlo se considerará inadecuado y los riesgos relacionados se informarán al empleado y su Jefe inmediato.
- La red de internet que la organización pone a disposición de los empleados, independientemente de su relación contractual, podrá utilizarse para fines personales legítimos, siempre que no afecte el progreso del trabajo ni ponga en riesgo la seguridad de la información. (Ejemplo: Consultar cuenta bancaria)

9. Ingeniería Social y Phishing

- Los colaboradores nunca deberán divulgar información de la organización, detalles de contacto, u otros detalles de profesionales a terceros desconocidos sin autorización previa del jefe inmediato, sobre todo, información clasificada como “restringida”, “confidencial” o de “uso interno”.
- En el caso de enlaces, correo electrónico u otra comunicación, en la que el usuario no está seguro de su procedencia o seguridad se deberá buscar orientación y notificar inmediatamente Líder de área y seguridad.

	POLITICA		PAGINA	21 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

• Los colaboradores no deberán proporcionar su nombre o contraseña a través de ningún enlace, correo electrónico, llamada telefónica u otro método hasta que el solicitante este totalmente identificado y verificado.

10. Gestión de Dispositivos

Los dispositivos móviles incluyen todo tipo de computadoras portátiles, teléfonos celulares, smartphones, dispositivos USB, tarjetas de memoria y otros dispositivos móviles utilizados para almacenar, procesar y transferir datos.

Los colaboradores deberán tomar precauciones cuando el dispositivo móvil se encuentra en automóviles u otro tipo de transporte, espacios públicos, habitaciones de hotel, lugares de reunión, centro de conferencias y otras áreas no protegidas fuera de las instalaciones de la organización.

Los colaboradores, que retiren los dispositivos móviles de las instalaciones de Easy LM , deberán tomar estas consideraciones:

- Los dispositivos móviles que contienen información clasificada como “confidencial”, “restringida” o de “uso interno” no deberán dejarse desatendidos y, si es posible, bloqueados físicamente.
- Cuando se utilicen dispositivos móviles en lugares públicas, el usuario deberá tener cuidado de que los datos no sean leídos por personas no autorizadas.
- La conexión a las redes de comunicación de la organización y el intercambio de datos deberá reflejar la confidencialidad de los datos y ser realizado a través del acceso VPN.

11. Uso de dispositivos removibles

Los puertos USB de las estaciones de trabajo y laptops se encuentran deshabilitados por razones de seguridad. Para aquellos escenarios donde se requiere hacer el uso de los mismos, se deberá de especificar los motivos y brindar una autorización del Jefe o Gerente inmediato.

12. Uso de laptop

En caso de daño, pérdida o no devolución de laptops y/o sus accesorios, el usuario se registrará bajo las políticas del Área de Recursos Humanos, el cual definirá el valor de indemnización correspondiente según sea el caso.

El usuario tendrá prohibido usar las estaciones de trabajo o laptops para cualquier otro propósito que no sea el relacionado con las actividades laborales de la organización.

13. Cuidado de los equipos

El usuario será responsable del almacenamiento del dispositivo mientras está en su posesión, teniendo cuidado de preservar el dispositivo, evitando su exposición en entornos y situaciones que pueden afectar sus mecanismos de funcionamiento.

A modo de ejemplo, aquí hay algunas precauciones especiales para garantizar la conservación de su equipo:

- No limpiar la pantalla portátil con alcohol o productos equivalentes. La limpieza deberá hacerse preferiblemente con una franela.

	POLITICA	PAGINA	22 de 1
	ANEXOS POLITICA GLOBAL	CA-PO015	
		VERSION	1

- No dejar caer líquidos sobre el teclado. Los líquidos deberán permanecer alejados de su equipo.
- No conectar la computadora portátil a una toma de corriente sin verificar primero y asegurarse que tenga el voltaje adecuado.
- No forzar o conectar cables opcionales sin saber primero que son compatibles, evitando así daños a un puerto físico de su computadora portátil.
- No colocar objetos pesados encima del teclado.
- No golpear o dejar caer su dispositivo asignado (incluyendo hand helds, laptops, tablets y celulares, en otros).
- Mantenga su dispositivo, así como sus cables o accesorios, en un lugar seguro y apropiado para evitar accidentes con las personas o con el dispositivo.

14. Gestión de Dispositivos

El trabajo remoto significa que los dispositivos portátiles o de comunicación se utilizarán para permitir que los usuarios trabajen fuera de las instalaciones de Easy LM, la concesión de acceso remoto deberá seguir el mismo proceso de gestión de acceso.

- La protección física de los dispositivos móviles.
- La prevención del acceso no autorizado por parte de personas que viven o trabajan en el lugar donde se realiza la actividad del trabajo remoto.
- La configuración de red adecuada utilizada para conectarse a Internet, bajo una red segura protegida por contraseña.

15. Obligaciones

Los usuarios tendrán responsabilidades explícitas de seguridad de la información y deberán ser responsables de sus acciones. Parte del rol general de la administración será monitorear el cumplimiento de los requisitos de la presente política:

- Cada empleado tendrá la obligación de proteger la información de propiedad o en custodia de Easy LM SAS y clasificarla correctamente de acuerdo con lo establecido con las políticas; así como proteger físicamente los activos.
- En caso de dañar físicamente algún dispositivo, se le solicitará un informe del incidente suscitado (en caso necesario).
- Todos los empleados, contratistas, proveedores y aliados de negocio tendrán la responsabilidad continua de proteger la información patentada por Easy LM SAS, los datos, los elementos de infraestructura y los sistemas de soporte, y de garantizar la seguridad, la confiabilidad e integridad de las actividades de procesamiento de información y procesamiento de información patentada.
- Las violaciones de cualquiera de los elementos anteriores deberán ser reportadas al líder de Seguridad y gerencias de área de la organización.

16. Penalidades

La organización se reserva el derecho de aplicar sanciones administrativas, legales y penales debido al asunto. Todos los colaboradores deberán garantizar el cumplimiento y la divulgación de las instrucciones

	POLITICA		PAGINA	23 de 1
	ANEXOS POLITICA GLOBAL		CA-PO015	
			VERSION	1

contenidas en las políticas y regulaciones de EASY LM SAS y, para no ser cómplices de ningún delito, deberán informar de inmediato cualquier violación de alguna regla a su superior inmediato y al Líder de seguridad, evitando que se conviertan en copartícipe del mismo grado de responsabilidad que el infractor.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN	APROBADO
0	13/05/2021	Emisión de documento	<i>John Arenas</i>
1	26/05/2022	Inclusión política uso aceptable de activos	

APROBACION

ELABORO		APOYO Y REVISO		APROBO	
SOFIA TULA		<i>Jhon Anaya</i>		<i>John Arenas</i>	
FECHA	26/05/2022	FECHA	26/05/2022	FECHA	26/05/2022