POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
VERSIÓN 1 JULIO DE 2023	DIVINA MIA SAS. NIT. 901.502473-3	

DIVINA MIA SAS., se encuentra comprometida con los valores de respeto, sujeción a la legalidad, reserva, confidencialidad, disponibilidad, integridad y manejo adecuado de la información y en especial con la convicción en la garantía de los derechos fundamentales. Por medio de la presente política, pretende dar cumplimiento a la ley 1581 de 2012, reglamentada por el Decreto 1377 de 2013, dentro de las cuales se destaca la necesidad de adoptar un Manual de Políticas y Procedimientos que garanticen el cumplimiento de dicha ley, atendiendo a las consultas y reclamos que surjan por parte del titular de los datos personales.

El Derecho a la Protección de los Datos Personales de cada titular se extiende desde saber quién conserva dichos datos y que uso se le está dando a los mismos, hasta de definir quién tiene la posibilidad de consultarlos.

La ley atribuye el poder a cada titular de consultar, modificar, suprimir y reanudar dicha información, y desarrolla las garantías e instrumentos para garantizar la vigencia del derecho fundamental.

El objeto de esta Manual es consagrar las Políticas Internas que habrán de fijarse en cumplimiento de la Ley 1581 de 2012 y que, por la condición de responsables del tratamiento de datos personales, debemos instrumentar y organizar a fin de cumplir a entera cabalidad con las disposiciones contempladas en la ley.

ALCANCE. - Las políticas de seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por el personal de la empresa o tengan relación con DIVINA MIA SAS., para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Dispositivos Móviles: DIVINA MIA SAS., proveerá las condiciones y limitaciones para el manejo de los dispositivos móviles (teléfonos inteligentes y tabletas, entre otros) institucionales. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos al interior de la empresa.

Los funcionarios o empleados directamente vinculados a la empresa y que ejerzan funciones administrativas, deben establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles que sean usados en ejercicio de sus funciones al interior de la empresa. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

Se debe configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

Igualmente, se debe instalar un software de antivirus tanto en los dispositivos móviles institucionales, siempre que esto sea posible y necesario.

El personal debe evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

El personal no debe modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

El personal debe evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

También se debe, cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

Se debe evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

El personal de la empresa debe evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

El personal no debe almacenar vídeos, fotografías o información personal en los dispositivos móviles institucionales asignados.

Todos los computadores usados por el personal de la empresa deben contar con la activación de los Firewall.

POLÍTICA PARA CONEXIONES REMOTAS. - El personal de la empresa que realice alguna conexión remota debe contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de DIVINA MIA SAS. y debe acatar las condiciones de uso establecidas para dichas conexiones

Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

POLÍTICA DE RESPONSABILIDAD CON LOS ACTIVOS. - DIVINA MIA SAS. P.H como propietaria de la información física, así como de la información generada, procesada y almacenada en su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad de la empresa, son activos de la entidad y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos del giro normal de sus actividades.

Toda la información sensible, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados.

POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN. – DIVINA MIA SAS., definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad y prioridad. Toda la información debe ser identificada, clasificada y documentada de acuerdo con las destinaciones específicas de los datos personales.

POLÍTICA DE USO DE PERIFÉRICOS. - El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de DIVINA MIA SAS., será reglamentado por la Gerencia de la empresa, considerando las labores realizadas por los funcionarios y su necesidad de uso. La empresa debe establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica.

También debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la empresa, de acuerdo con los lineamientos y condiciones establecidas.

La empresa debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la empresa, ya sea cuando son dados de baja o reasignados a un nuevo usuario.

Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la empresa.

Los funcionarios y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la empresa.

Los funcionarios y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados.

Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica.

POLÍTICAS DE ACCESO A REDES Y RECURSOS DE RED.- La empresa, como responsables de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

El personal de la empresa, debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red.

También se debe asegurar que las redes inalámbricas de la empresa cuenten con métodos de autenticación que evite accesos no autorizados.

Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la empresa deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS. - DIVINA MIA SAS., establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la empresa. Asimismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

La Gerencia, debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la entidad, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

La empresa debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido. Igualmente, debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

También debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de DIVINA MIA SAS. deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la empresa deben acogerse a lineamientos para la configuración de contraseñas implantados por la entidad.

POLÍTICA DE CONTROLES CRIPTOGRÁFICOS. - DIVINA MIA SAS., velará porque la información general, clasificada como reservada o restringida; será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

DIVINA MIA SAS. S.A.S debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.

Igualmente debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos. Se debe desarrollar y establecer un procedimiento para el manejo y la administración de cifrado.

La empresa debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

POLÍTICA FRENTE A SOFTWARE MALICIOSO. - DIVINA MIA SAS., proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena; adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

La empresa debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso. Igualmente debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio. Se debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus.

La empresa, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware. Igualmente debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por La Dirección de Sistemas; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

El personal de la empresa debe asegurarse de que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y

seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

El personal que sospechen o detecten alguna infección por software malicioso deben notificar a la Dirección de Sistemas, para que, a través de ella, se tome las medidas de control correspondientes.

POLÍTICA DE COPIA DE RESPALDO DE INFORMACIÓN.- DIVINA MIA SAS. genera copias de seguridad a los equipos administrativos que son alojadas en un sistema de almacenamiento en nube.

POLÍTICA DE SEGURIDAD EN INTERNET.- DIVINA MIA SAS. entendiendo la necesidad de internet como herramienta de trabajo proporcionará los recursos necesarios para asegurar su disponibilidad al personal administrativo de la empresa que así lo requiera para el desarrollo de sus actividades diarias.

La presente política fue actualizada por última vez en julio de 2023.