MANUAL DE SEGURIDAD DE LA INFORMACIÓN

Elaboró:	Revisó:	Aprobó:
		
Rogelio Barajas González	Miguel Angel Nova Salgado	Héctor Obregón Roa
Gerente Learning y Operations	Gerente de Calidad y Procesos	Director General

Sección de Cambios

Fecha	Revisión No.	Descripción	Iniciales, Firma y Fecha	
			Revisó	Aprobó
15-01-2018	00	Emisión del Original	MNS	HOR

INDICE

Tema **Pág.**

1. OBJETIVO

Establecer los lineamientos y controles necesarios para mantener la seguridad de la información propiedad del Cliente y/o sensibles para la Organización, a través de su identificación, almacenamiento, control de acceso, administración y disposición final.

2. ÁMBITO DE APLICACIÓN O ALCANCE

Es aplicable a todos los Colaboradores de la Organización que tienen acceso a los datos del Cliente y/o sensibles para la Organización, y a los involucrados en gestionar la seguridad de la información a través de la Gestión de la Confidencialidad de la Información, Gestión de Usuarios de Bases de Datos, Respaldos de información de las Bases de Datos, Disposición de Bases de Datos, Control de Acceso a los Servicios de Hosting de Microsoft (Azure) y Configuración de Accesos y Protección de Equipos y Cuentas.

3. PREMISAS GENERALES

1. El área de Calidad y Procesos debe programar y ejecutar auditorías que incluyan la revisión de los lineamientos de este Manual, de acuerdo con lo establecido en el **Programa de Revisiones Documentales y Auditorías Internas** del Sistema de Gestión de Calidad.

2. Cuando un área lo requiera, se debe programar y ejecutar la revisión de estos lineamientos por parte del Especialista de Seguridad de la Información, Gestión de Usuarios de Bases de Datos.

3. El área de Soporte Técnico debe configurar y revisar que se cumplan los lineamientos establecidos en la sección 7.7 de este Manual, previo a la entrega de cualquier equipo de cómputo (PC o MAC) de acuerdo con lo establecido en el **Procedimiento de Solicitud de Equipos**.

4. MARCO NORMATIVO

INTERNO

- Procedimiento de Control de Documentos.

EXTERNO

- N/A

5. ACTUALIZACIÓN

Es responsabilidad del Gerente de Learning y Operations la emisión y actualización de este Manual, así como de recibir propuestas de cambio. Este Manual se revisará y/o actualizará cada año o antes si se requiere.

6. DEFINICIONES

Información del Cliente:	Cualquier información de datos personales, vinculada o que pueda asociarse a las bases de datos que comparten las Empresas que contratan la prestación de servicios de Formiik.
Información sensible:	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
Convenio de Confidencialidad y No Divulgación:	Es un documento en la que los Colaboradores de la Organización manifiestan su voluntad de mantener la confidencialidad de la información de la Empresa o la provista por terceras partes, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de las actividades que desarrollan dentro de la misma.
Base de Datos:	Conjunto organizado de datos personales que sea objeto de tratamiento.
Autentificación:	Es el procedimiento de la comprobación de la identidad de un Usuario o recurso tecnológico, al tratar de acceder a un recurso de procesamiento o sistema de información.
Cifrado:	Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir el robo de información, el monitoreo y el acceso no autorizado a los repositorios de información.

7. DESARROLLO

7.1. FLUJO DE INFORMACIÓN DE LOS CLIENTES.

1. La plataforma tecnológica Formiik, está orientada a la optimización de cualquier proceso de negocio en campo, utilizando los servicios de hosting Microsoft (Azure) y a través de canales cifrados para la interconexión de los diferentes elementos que se comunican con la misma, con el objetivo de salvaguardar la información de los Clientes y las tareas ejecutadas. La información de los Clientes es utilizada de acuerdo con el siguiente flujo de operación de Formiik. Ver Figura 1.

   - La información de los Clientes, es administrada y controlada en los servidores centrales de la Empresa que contrata los servicios de Formiik.

   - La Empresa contratante, envía a Formiik la información necesaria para la ejecución de las tareas solicitadas (Agregar, Cancelar, Actualizar).

   - Formiik recibe la información del Cliente final, la registra y procesa (Enviar, Recibir, Actualizar, Entregar), para llevar acabo la tarea solicitada por la Empresa contratante, enviando la información del Usuario (autentificación y respuesta).

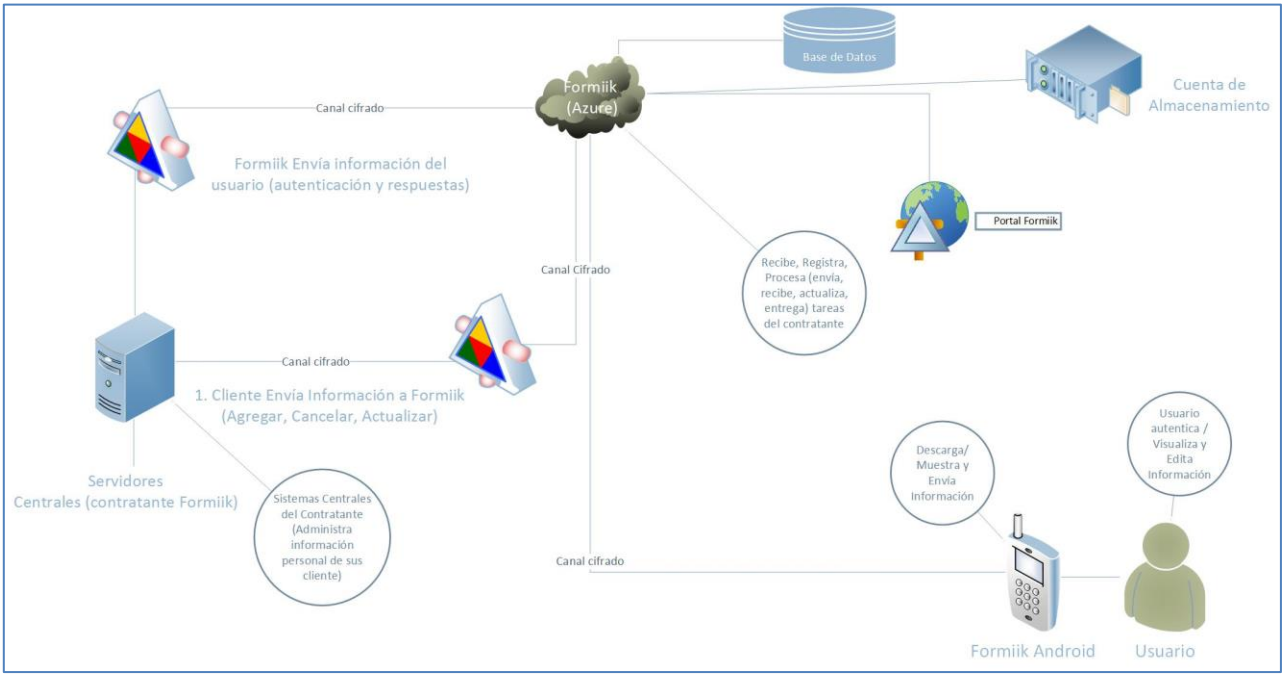

Figura 1

7.2. GESTIÓN DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN.

1. El área de Capital Humano debe entregar sin excepción alguna, el ***Convenio de Confidencialidad y No Divulgación*** a todos los Colaboradores nuevo ingreso durante el proceso de contratación, solicitando su lectura y firma correspondiente, el cual establece entre los puntos más importantes lo siguiente:

    - El Colaborador asume la obligación de guardar la más absoluta discreción estableciendo al efecto un pacto de confidencialidad y de no revelación o divulgación de la INFORMACIÓN que con motivo de su contrato de trabajo, maneja, desarrolla o implementa, por tratarse de datos personales, propiedad de "LA EMPRESA" o de los terceros a quienes dicha empresa presta servicios.

    - El Colaborador asume por virtud del Convenio, la obligación de no divulgar, publicar, revelar, imitar, transmitir, reproducir, modificar o hacer pública o de cualquier otra forma disponer de la INFORMACIÓN CONFIDENCIAL de "LA EMPRESA" o de los terceros a quienes dicha empresa presta servicios, mediante cualquier método posible para el uso o beneficio propio o de terceros, sin la previa autorización por escrito de la "LA EMPRESA".

    - El Colaborador reconoce que las claves de acceso que le han sido proporcionadas por "LA EMPRESA", o de los terceros a quienes dicha empresa presta servicios para el uso de los sistemas, para la gestión para la cual fue contratado, son de carácter personal e intransferible, por lo que no podrá cederla por ningún título o hacerse sustituir por terceros en la utilización de las mismas, por lo que es su obligación proteger la información y su buen uso.

    - El Colaborador se obliga a devolver cualquier información, documentación, antecedentes, equipo, claves o programas facilitados en cualquier tipo de soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del Convenio, en el supuesto de que cese la relación entre las partes por cualquier motivo.

    - El Colaborador se obliga a observar el presente convenio, hasta por 5 años posteriores a la terminación del contrato y relación de trabajo que le une con "LA EMPRESA", sea cual fuere la causa que motive la terminación del vínculo contractual.

    - El incumplimiento en cualquiera de sus partes del presente convenio, dará causa a la rescisión justificada del contrato de trabajo celebrado entre "EL EMPLEADO" y "LA EMPRESA" de conformidad con el artículo 47 de la Ley Federal del Trabajo.

7.3. GESTIÓN DE USUARIOS DE BASES DE DATOS.

Alta de Usuarios:

2. El Gerente de On Boarding, Engagement, Desarrollo y SQA debe solicitar el acceso a las Bases de Datos de los Clientes, únicamente para aquellos Colaboradores bajo su cargo y/o de nuevo ingreso que requieran el uso de las mismas para la ejecución de sus funciones. Esto debe realizarse a través del levantamiento de un ***Ticket en Zendesk***, detallando el nombre completo y correo electrónico del Colaborador correspondiente.

3. El Ingeniero N1 debe canalizar el ticket al Ingeniero N2, para que éste último lleve a cabo la configuración de los accesos en el servidor correspondiente de SQL y en la cual debe considerar las siguientes premisas.

AREA	PERMISO	AMBIENTE DE ACCESO
SQA	Lectura	RC y Desa
Desarrollo	Lectura	RC y Desa
Onboarding	Lectura	Producción
Engagement	Lectura	Producción
Learning	Lectura	Producción
Operations	Escritura	Producción

4. El Ingeniero N2 debe documentar en el ***Ticket de Zendesk*** el rol que se asignó al Colaborador, así mismo; debe requisitar y enviar la ***Carta Responsiva*** al mismo, solicitándole su firma correspondiente.

5. El Colaborador debe firmar la ***Carta Responsiva*** en un plazo no mayor a 24 horas de haberla recibido y hacerla llegar de manera escaneada al Ingeniero N2.

6. El Ingeniero N2 debe monitorear que el Colaborador correspondiente, regrese la Carta Responsiva firmada en tiempo y forma, de lo contrario deberá bloquear el acceso a la Base de Datos, y desbloquear el mismo hasta que reciba la ***Carta Responsiva*** firmada.

7. El Ingeniero N2 debe resguardar la ***Carta Responsiva*** en Google Drive / Carpeta Operations e informar al Gerente de Operations la configuración del acceso realizado a las Bases de Datos correspondientes.

8. El Gerente de Operations debe verificar a través de la inspección al azar de 2 Colaboradores de forma mensual, que los permisos asignados para su acceso a las bases de datos estén correctos, en caso de que identifique inconsistencias, se debe verificar los motivos de las mismas, si en la investigación se detecta que la inconsistencia fue con dolo por parte del Colaborador, se debe remitir el caso a RRHH para la firma de la ***Acta Administrativa*** por mala práctica. En caso de que la inconsistencia no haya sido con dolo, se debe de retroalimentar al Colaborador en cuestión y monitorear que no vuelva a suceder.

Baja de Usuarios:

1. Cuando un Colaborador con acceso a las bases de datos vaya a causar baja, el Gerente de On Boarding, Engagement, Desarrollo y SQA, debe solicitar la baja del acceso a las bases de datos correspondientes, por lo menos con 24 hrs., de anticipación a la salida del Colaborador. Esto debe realizarse a través del levantamiento de un ***Ticket en Zendesk***, detallando el nombre completo y correo electrónico del Colaborador correspondiente.

2. El Ingeniero N1 debe canalizar el ticket al Ingeniero N2, para que éste último lleve a cabo la baja de los accesos del Colaborador en el servidor correspondiente de SQL.

3. El Ingeniero N2 debe documentar en el ***Ticket de Zendesk*** la actividad realizada y cerrar el mismo, así mismo; debe ingresar a la Google Drive / Carpeta Operations y borrar la ***Carta Responsiva*** del Colaborador correspondiente.

7.4. RESPALDOS DE INFORMACIÓN DE LAS BASES DE DATOS.

1. El Ingeniero N2, debe llevar a cabo el respaldo de la información de las bases de datos nuevas, ingresando a la herramienta de Azure Explorer en el apartado de Base de Datos SQLS y seleccionando la opción de “Base de Datos Nueva”, posteriormente; debe configurar el respaldo de la información de acuerdo con los siguientes pasos:
    - Selecciona el estado de la configuración en automático, y elije la cuenta de “Almacenamiento Backup”.
    - Elije la Frecuencia “diario” y el Horario “A media noche”.
    - Define en Retención como plazo “15 días”.

2. En el caso de bases de datos existentes, la herramienta Azure Explorer, corre automáticamente el proceso de respaldo de información, de acuerdo con la configuración realizada previamente.

3. El Ingeniero N2 debe verificar todos los días lunes, que los respaldos de información configurados se estén ejecutando en tiempo y forma. Para esto ingresa a Visual Estudio, sección Azure Explorer y verifica las cuentas de “Formiik Backup” y “Automated Export”. En caso de que se detecté un error, debe realizar el respaldo de forma manual e ingresar a la configuración de respaldo y para asegurarse que ésta se encuentre activa.

4. El Ingeniero N2, todos los días lunes toma el respaldo más reciente de las bases de datos y lo copia a la cuenta de Backup Mont y genera un ***Ticket Zendesk*** para evidenciar las tareas de respaldo realizadas.

7.5. DISPOSICIÓN DE BASES DATOS.

1. Cuando se concluya la relación comercial con la Empresa que contrató la prestación de servicios de Formiik (Cliente) o cuando ésta lo solicita, se debe llevar acabo la disposición de las bases de datos compartidas por el Cliente, dependiendo si éstas se encuentran en un storage compartido o privado.

Storage compartido:

- El Ingeniero N2 debe ingresar al servidor correspondiente donde se almacena la(s) base(s) de datos del Cliente y elimina la(s) misma(s) ejecutando las instrucciones de deletes específicas. Como evidencia de la actividad, se debe de obtener un screen inicial (donde se visualice la existencia de la(s) base(s) de datos) y un screen final (donde se visualice que la(s) base(s) de datos ya no existe en el servidor).

- El Ingeniero N2 debe documentar en el ***Ticket de Zendesk*** la actividad realizada y cerrar el mismo, así mismo; debe compartir vía correo electrónico los screens al Cliente, como evidencia de la disposición final de su(s) base(s) de datos.

Storage privado:

- El Ingeniero N2 debe ingresar al servidor correspondiente donde se almacena la(s) base(s) de datos del Cliente y borra la(s) misma(s). Como evidencia de la actividad, se debe de obtener un screen inicial (donde se visualice la existencia de la(s) base(s) de datos) y un screen final (donde se visualice que la(s) base(s) de datos ya no existe en el servidor).

- El Ingeniero N2 debe documentar en el ***Ticket de Zendesk*** la actividad realizada y cerrar el mismo, así mismo; debe compartir vía correo electrónico los screens al Cliente, como evidencia de la disposición final de su(s) base(s) de datos.

2. Para la disposición de la(s) base(s) de dato(s) que fueron respaldadas de acuerdo con lo establecido en el punto 7.4. de este Manual, se debe realizar lo siguiente.

- El Ingeniero N2 debe ingresar a Visual Estudio, sección Azure Explorer y eliminar la(s) base(s) del Cliente que tengan respaldadas en “Formiik Backup”. se debe de obtener un screen inicial (donde se visualice la existencia de la(s) base(s) de datos) y un screen final (donde se visualice que la(s) base(s) de datos ya no existe en el servidor).

- El Ingeniero N2 debe documentar en el ***Ticket de Zendesk*** la actividad realizada y cerrar el mismo, así mismo; debe compartir vía correo electrónico los screens al Cliente, como evidencia de la disposición final de su(s) base(s) de datos.

7.6. CONTROL DE ACCESO A LOS SERVICIOS DE HOSTING MICROSOFT (AZURE).

1. Los controles establecidos para el acceso y/o suscripción a los servicios de hosting Microsoft (Azure), solo deben estar configurados a cuentas corporativas y a los siguientes roles sin excepción alguna:
    - Gerente de Producto.
    - Líder de Desarrollo Web.
    - Gerente de Learning y Operations.
    - Ingeniero N2.
    - Director General.

2. El Gerente de Producto, Líder de Desarrollo Web, Gerente de Learning y Operations, Ingeniero N2 y Director General, deben activar la conexión a través del medio de autentificación por doble factor.

3. El control de accesos vía remota, debe ser a través de un firewall administrado en los servicios de hosting Microsoft (Azure), y con restricciones de acceso solo para IP´s autorizadas.

7.7. CONFIGURACIÓN DE ACCESO Y PROTECCIÓN DE EQUIPOS Y CUENTAS.

Premisas:

1. El área de Soporte Técnico debe configurar y revisar que se cumplan los lineamientos establecidos en esta sección, previo a la entrega de cualquier equipo de cómputo (PC o MAC) de acuerdo con lo establecido en el **Procedimiento de Solicitud de Equipos**.

Equipos PC´s:

1. Todo equipo debe contar con la Autenticación por cuenta de Microsoft, para el inicio de sesión. Ver Figura 2.

2. Todo equipo debe tener instalado Windows Defender, con las actualizaciones automáticas activas. Ver Figura 3.

Figura 2

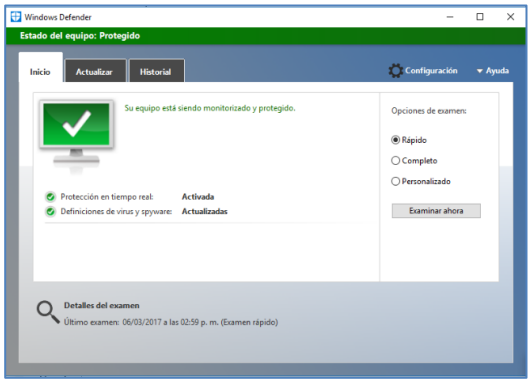

Figura 3

3. A todo equipo se le debe configurar desde Ahorro de Energía, el bloqueo de pantalla por inactividad de 2 minutos, con solicitud de contraseña Microsoft para desbloqueo. Ver Figuras 4 y 5.

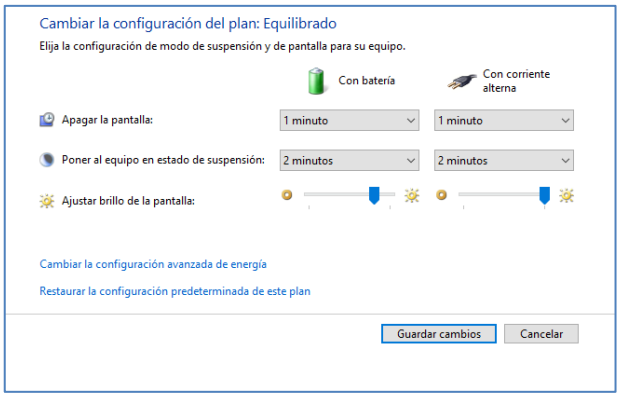

Figura 4

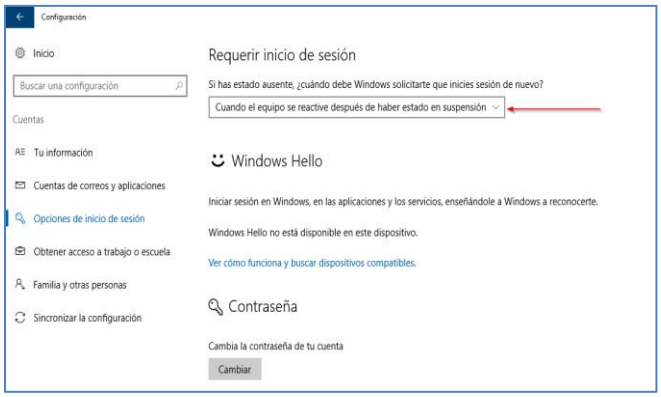

Figura 5

Equipos MAC's:

1. Todo equipo debe contar con la Autenticación por cuenta de Microsoft para el inicio de sesión. Ver Figura 6.

2. A todo equipo se le debe deshabilitar la opción de "Login Automático". Ver Figura 7.

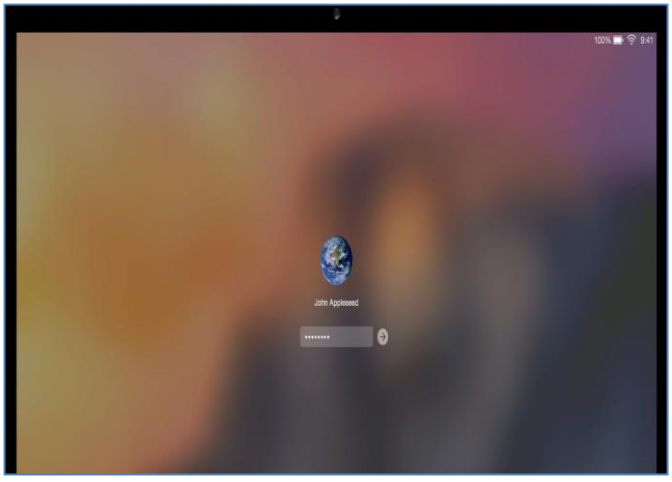

Figura 6

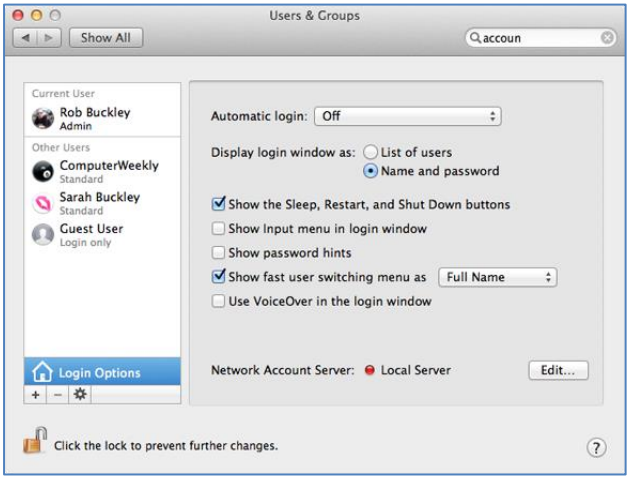

Figura 7

3. A todo equipo se le debe configurar desde Ahorro de Energía, el bloqueo de pantalla por inactividad y con solicitud de contraseña de forma inmediata. Ver Figura 8.

Figura 8

Cuentas de Google:

1. A toda cuenta con dominio formiik.com, se debe configurar la autenticación por doble factor, incluyendo la complejidad estándar de contraseñas. Ver Figura 9.

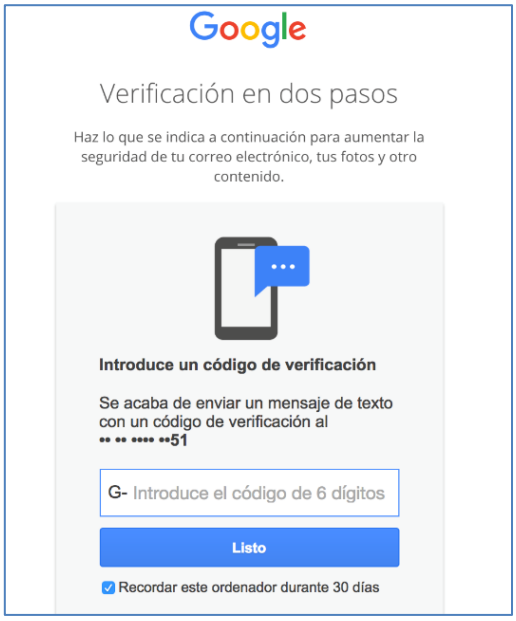

Figura 9.

Cuentas de Microsoft:

1. Toda cuenta utilizada para autenticar con Azure, debe tener activa la certificación por doble factor. Ver Figura 10.

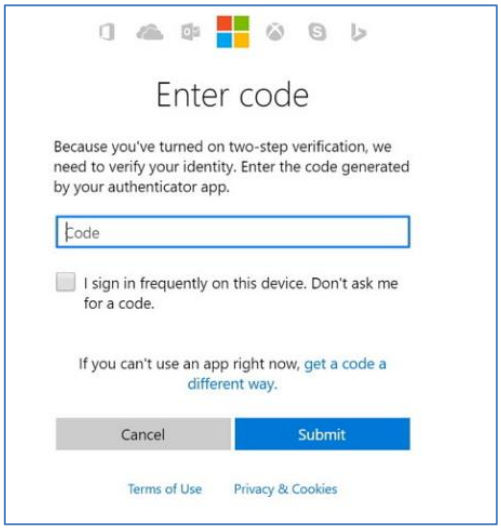

Figura 10.

Cuentas de Apple:

1. Toda cuenta utilizada para autenticar en el equipo, debe tener activa la certificación por doble factor. Ver Figura 11.

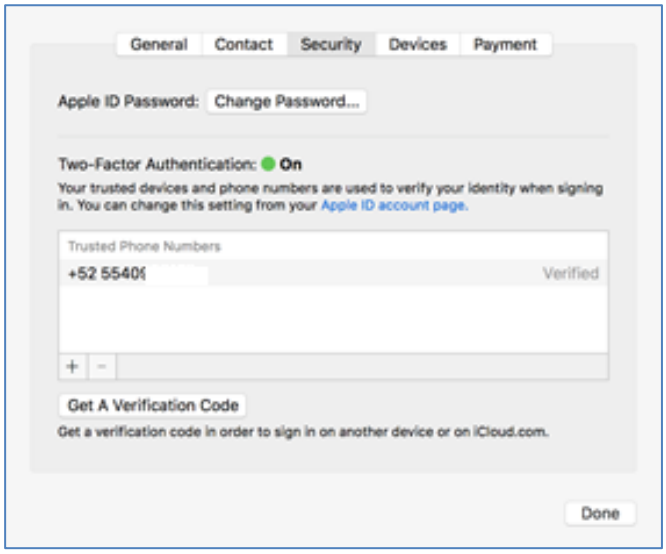

Figura 11.

8. REGISTROS

El Gerente de Learning y Operations es responsable de conservar e ir actualizando los registros generados en este Manual.

Los registros obsoletos de este Manual, se conservarán por un periodo mínimo de un año, al término de este periodo serán destruidos o eliminados.

Registros:

Título	Responsable	Tipo de almacenamiento	Tiempo de retención	Disposición Final
Convenio de Confidencialidad y No Divulgación	Bullincome	Electrónico / Google Drive	Duración del Contrato	Backup
Ticket en Zendesk	Ingeniero de Soporte N2	Electrónico / Zendesk	1 año	Backup
Carta Responsiva	Gerente de Learning y Operations	Electrónico / Drive / Carpeta Operations	Mientras el colaborador este vigente	Eliminación
Acta Administrativa	Coordinador de Capital Humano / Analista de Capital Humano	Expediente del Colaborador	Duración del Contrato	Eliminación