TRATAMIENTO DE DATOS PERSONALES A TRAVÉS DE DISPOSITIVOS INFORMÁTICOS

## REGISTRO ACTIVIDAD DE TRATAMIENTO

De conformidad con el Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016 y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, le informamos de que los datos de carácter personal facilitados en el presente serán incorporados en un fichero titularidad y responsabilidad de ${razon}

|  |  |
| --- | --- |
| RESPONSABLE DEL TRATAMIENTO DE DTAOS PERSONALES | ${razon} |
| ${domicilio} |
|
| ${email} |
| FINALIDAD DEL TRATAMIENTO | Desarrollo de la actividad laboral.  Ejercer funciones de control, de acuerdo con lo establecido en el artículo 20.3 del Estatuto de los Trabajadores |
| CATEGORÍA DE INTERESADOS | Empleados. Personal que presta servicios en la organización de la entidad, para lo cual cede sus datos personales. |
| CATEGORÍA DE DATOS | Los necesarios para el mantenimiento de la relación laboral  Se tratarán datos como: nombre, apellidos, número de Seguridad Social, dirección, teléfono de contacto, correo electrónico. Datos profesionales y académicos |
| DESTINATARIOS | Administración Tributaria. Cuerpos y fuerzas de seguridad del Estado. Bancos y entidades financieras. Otros destinatarios. |
| TRANSFERENCIAS DE DATOS CON CARÁCTER INTERNACIONAL | ${transferencas} |
| PLAZO DE CONSERVACIÓN | Se conservarán los datos durante el tiempo necesario para cumplir con la finalidad para la que se recabaron.  Una vez desaparezcan las finalidades para las que han sido recabados los datos inicialmente, estos se conservarán los términos previstos en la legislación para el cumplimiento necesario respecto a la prescripción de responsabilidades |

MEDIDAS DE SEGURIDAD PARA EL TRATAMIENTO DE DATOS PERSONALES A TRAVÉS DE DISPOSITIVOS INFORMÁTICOS

**NORMAS Y PROCEDIMIENTOS DE SEGURIDAD**

El Responsable del Tratamiento ha establecido las siguientes normas y procedimientos de seguridad, de obligado cumplimiento, por parte de todo el personal:

**Uso adecuado de los recursos de la organización referentes a:**

Dispositivos tecnológicos que el Responsable del Tratamiento pone a disposición del personal.

Las Tablets, Ordenadores de Sobremesa, Portátiles, Móviles, Teléfonos Inteligentes como cualquier otro dispositivo que sirva para el tratamiento, transporte y/o almacenaje de información que el Responsable del Tratamiento ponga a disposición del personal para realizar su trabajo, deberán ser custodiados por la persona al cual se haya asignado, debiendo dicha persona cumplir con todas las medidas de seguridad que vengan impuestas por la empresa.

Dichos dispositivos no podrán emplearse con fines ajenos a la actividad laboral. Si el trabajador o la trabajadora necesitan utilizarlo con fines ajenos a la actividad laboral, deberán contar con la autorización previa y por escrito de la organización.

Cuando se utilicen los equipos fuera del centro de trabajo, queda prohibido conectarse a redes WiFi públicas o de acceso gratuito y dejar el equipo desprotegido, debiendo en todo momento estar pendiente del mismo.

Internet y redes WIFI.

Todo el personal debe procurar un uso seguro y legal, tanto de Internet como de las redes WiFi de la organización, por lo cual, bajo ningún pretexto podrán:

* Acceder a páginas web que supongan una actividad ilegal, o de contenido no relacionado con el trabajo, así como también el acceso a páginas de dudosa procedencia.
* Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma, material ilegal, como, por ejemplo: pornografía (de cualquier tipo); material amenazante, fraudulento, discriminatorio, difamatorio, ofensivo, obsceno, insultante o contrario a la moral y las buenas costumbres.
* Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma material de cualquier tipo que esté protegido por el secreto comercial o por patentes vigentes.
* Transmitir, visualizar, editar, copiar, compartir, descargar y/o manipular de cualquier forma cualquier archivo de tipo musical, de lectura o filmográfico, sin tener los derechos de propiedad intelectual correspondientes.
* Escanear o probar la vulnerabilidad de equipos, sistemas o segmentos de red.
* Enviar mensajes no solicitados, cualquier tipo de virus, código malicioso o ataques internos o externos a la red.
* Dañar de cualquier forma equipos, sistemas informáticos o redes y/o perturbar el normal funcionamiento de la red, tanto de la organización como de terceros.
* Interceptar, recopilar o almacenar datos sobre terceros que no estén relacionados con la actividad laboral y sin su conocimiento y consentimiento expreso.
* Obtener acceso no autorizado a equipos, sistemas o programas tanto dentro como fuera de la red.
* Conectarse a la red reservada para invitados.
* Conectarse a redes públicas.
* Realizar cualquier otro tipo de acción, tanto de forma directa como indirecta, que ponga en riesgo la disponibilidad, integridad y/o confidencialidad de la información, como la seguridad e integridad de los sistemas que utiliza la organización.

Terminales y líneas telefónicas.

Los terminales, tanto fijos como móviles, tarjetas SIM y líneas telefónicas contratadas, no pueden utilizarse para fines ajenos a los relacionados con la actividad laboral que el personal desempeña para el Responsable del Tratamiento.

Solamente podrán utilizarse para fines personales, los equipos señalados, en caso de emergencia familiar, aunque en ningún caso podrán almacenarse en los mismos datos personales que puedan individualizar a una persona.

Queda también prohibido la manipulación de los terminales para lograr privilegios superiores a los otorgados por la organización, grabar llamadas, duplicar tarjetas SIM y en general cualquier actividad contraria.

Correo electrónico.

Ud. es el principal responsable del correcto uso de la cuenta de correo electrónico profesional que se le asigna, por lo cual deberá cumplir con las siguientes obligaciones:

* Está prohibido el envío de correos electrónicos con en el que se adjunten bases de datos personales o bien se copie el contenido de las mismas dentro del cuerpo del correo electrónico. Si, por razones del trabajo que se desarrolla, debe enviarse este tipo de información, la misma deberá enviarse únicamente mediante un archivo adjunto y dicho archivo deberá estar cifrado, la clave, en ningún caso se transmitirá por correo electrónico.
* Está prohibido enviar o reenviar mensajes en cadena o con fines comerciales o publicitarios sin el consentimiento expreso del destinatario.
* Está prohibido configurar la cuenta de correo electrónico profesional en cualquier dispositivo sin la autorización previa y por escrito de la dirección.
* Está prohibido permitir el acceso al contenido de su cuenta de correo electrónico profesional a cualquier persona, ya sea personal interno como externo de la organización; sólo podrán tener acceso a su contenido a quien la dirección indique y por razón fundada.
* No podrá utilizar su cuenta de correo personal, bajo ningún pretexto, para la realización de la actividad laboral.
* El correo electrónico corporativo solo podrá ser utilizado para los fines correspondientes a la actividad laboral y en ningún momento con fines propios o privados quedando totalmente prohibido el envío o la recepción de correos ajenos a las funciones laborales con contenido personal.
* Se advierte que para el envío de un correo electrónico a varias personas, se debe utilizar la casilla CCO (con copia oculta) ya que en caso contrario se podría entender que se vulnera el deber de secreto.
* En todo caso, se informa a los empleados de que la entidad podrá acceder al correo en caso de considerarlo necesario.

Política de escritorios limpios.

Si no te encuentras en tu puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos, que contengan información que puedan contener datos personales, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

Este tipo de documentos y soportes deben ser archivados de forma segura.

Tu puesto de trabajo debe estar limpio y ordenado; podrás disponer únicamente de los activos que hemos puesto a tu disposición.

No podrás tener recipientes ni envases sobre tu mesa de trabajo, cuyo cierre no sea hermético y que contengan líquidos, con el fin de evitar su vertido encima de los equipos informáticos y/o cualquier otro tipo de soporte que pueda verse afectado por el vertido.

Política de pantallas limpias.

La ubicación de los puestos de trabajo y la colocación de las pantallas está organizada de tal forma que sólo la persona que utiliza la misma puede leer lo que se plasma en la pantalla, evitando miradas indiscretas.

Si la persona autorizada no se encuentra en su puesto de trabajo, debe quitar toda la información sensible de la pantalla y bloquear el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas o bloqueando la pantalla mediante el uso de la siguiente combinación de teclas:

*Botón Windows + L*

Si la persona se ausenta por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se implementa finalizando la sesión en todos los sistemas y apagando el ordenador.

Política de contraseñas.

El personal tiene prohibido divulgar, compartir y/o entregar, tanto a personal interno como externo de la organización, las contraseñas que tengan para acceder tanto a los sistemas informáticos, programas, como a las Bases de Datos que contengan datos de carácter personal.

Al momento de crear la contraseña, deberá tener en cuenta lo siguiente:

* La contraseña deberá tener, al menos, 15 caracteres. No obstante, el número de caracteres es optativo de cada organización, la razón de la extensión es que cuantos más dígitos tenga la contraseña, más difícil es romperla por un ataque de fuerza bruta si se consigue su hash.
* Deberán combinarse letras mayúsculas y minúsculas, números y símbolos.
* No podrá utilizar la misma contraseña en diferentes servicios.
* No podrá utilizar aquellas contraseñas que utilice en su vida privada, por ejemplo, la de acceso al banco, a su cuenta de red social, etc.
* No podrá reutilizar contraseñas que ya haya utilizado previamente.
* No podrá utilizar patrones de teclado, por ejemplo: “qwerty” o “uiop” o “1qaz” “2wsx” o “3edc” ni la combinación de estas.
* Las contraseñas tienen un período de vigencia de 3 meses. No obstante, el tiempo es optativo de cada organización, la razón de los 3 meses es que no todos los ataques van dirigidos a ser descubiertos ni a encriptar o destruir una base de datos en particular, existen ataques que tienen como fin recabar la mayor cantidad de información posible, por lo cual, si se cambia la clave cada 3 meses, la perdida de confidencialidad estará acotada a un tiempo menor.
* Una vez creada la contraseña, deberá asegurar su correcta gestión y almacenamiento, por lo cual, deberá seguir las siguientes directivas:
* No apuntar la contraseña en notas y pegarlas en el escritorio, pantalla u ordenador.
* No utilizar la opción de “recordar contraseña” que ofrecen los navegadores.
* No almacenar la contraseña, dentro de su ordenador, en archivos sin cifrar y que estén a la vista de cualquier usuario y que lleven nombres que permita su fácil identificación, por ejemplo: “listado de contraseñas”, “contraseñas”, “pass”, “password”, etc.

**Sobre la instalación por parte del personal laboral de programas por cuenta propia.**

El personal no puede instalar ningún tipo de software por cuenta propia sin la autorización previa y por escrito del Responsable del Tratamiento.

En el caso que el trabajador/a proceda sin autorización ni conocimiento por parte de la organización del Responsable del Tratamiento, el trabajador/a quedará vinculado y será́ responsable en caso de daños ocasionados al equipo informático y/o a la información en él contenida como consecuencia de dicha instalación.

Antes de instalar un programa, el personal autorizado deberá comprobar que se cuenta con la licencia y derechos de uso del programa; con la certificación del programa para su compatibilidad con el sistema operativo y los demás aplicativos; con la garantía del código para evitar posible presencia de virus, troyanos y otros programas espías.

En todos los casos, cualquier tipo de software que se instale, deberá mantenerse actualizado siguiendo las indicaciones del desarrollador del software en cuestión.

Pruebas con datos reales.

Las pruebas anteriores a la implantación y/o modiﬁcación de los sistemas de información que traten ﬁcheros con datos de carácter personal no se realizarán con datos reales.

En el caso de resultar necesario utilizar datos reales con el fin de poder realizar la prueba de forma positiva, deberá asegurarse el nivel de seguridad correspondiente al tipo de tratamiento y a los datos de carácter personal afectados para que los mismos no sean objetos de una brecha de seguridad.

**Control de accesos.**

El personal sólo puede acceder a los datos y dependencias que sean necesarios para el correcto desarrollo de sus funciones.

Entrada y salida de las instalaciones de la organización

Existe implantado en la organización un sistema de control de accesos cuyo objetivo es la identiﬁcación de personal, con el fin de evitar el ingreso de personas ajenas a la organización y el registro de jornada horaria con el fin de controlar y monitorizar el flujo del personal de la entidad.

Despachos

Aquellos despachos que disponen de una puerta con llave, son sus ocupantes los encargados de que permanezcan cerrados cuando finalice la jornada laboral o se ausenten de su puesto de trabajo.

Todos los despachos que dispongan de armarios y cajoneras con llaves, siendo aquellas personas que los utilizan, las encargadas de que permanezcan cerrados cuando finalice la jornada laboral o se ausente de su puesto de trabajo.

Es responsabilidad de quienes tengan asignadas llaves, la custodia de las mismas al igual que la comunicación de su extravío al Responsable del Tratamiento, Delegado de Protección de Datos (si estuviera designado) o a aquella persona que designe el Responsable del Tratamiento.

Queda prohibido realizar copias de las llaves al igual que distribuir las mismas sin autorización expresa del Responsable del Tratamiento. Tampoco se podrá ceder o prestar las mismas a terceras personas sin autorización expresa del Responsable del Tratamiento.

Cuarto del servidor

Únicamente el Responsable de Seguridad, el Delegado de Protección de Datos (si estuviera designado) y/o el personal autorizado por el Responsable del Tratamiento, están autorizados para acceder a las dependencias en las que se encuentren los sistemas de información que corresponden al servidor y a las copias de respaldo.

Es responsabilidad de quienes tengan asignadas claves de acceso, la custodia de las mismas al igual que la comunicación de su filtración al Responsable del Tratamiento, Delegado de Protección de Datos (si estuviera designado) o a aquella persona que designe el Responsable del Tratamiento.

**Régimen de trabajo fuera de los locales de la organización:**

El tratamiento de datos de carácter personal, fuera de los locales de la organización, deberá ser autorizado expresamente por el Responsable del Tratamiento, teniéndose en consideración las funciones que realiza el personal en la organización.

En el caso de que se autorice el tratamiento de datos fuera de los locales de la organización, el personal que los trate, deberá cumplir con todas las medidas de seguridad indicadas en los puntos 5.1 y 5.3 del presente documento y con todas aquellas que establezca la organización para el caso concreto.

**Copias de respaldo y recuperación**.

La organización realiza copias de seguridad de forma habitual y sistemática, por lo cual es su responsabilidad acatar las indicaciones que vengan impartidas por el departamento informático de la empresa.

**Gestión de soportes.**

Utilización de soportes extraíbles.

Por regla general, el personal no podrá disponer fuera de la entidad de ningún soporte con datos de carácter personal en los que la entidad actúe como Responsable o Encargada del Tratamiento.

El personal laboral que lo desee deberá solicitar una autorización previa para el tratamiento de datos en relación con las salidas y/o entradas de soportes del centro de trabajo.

Únicamente el Responsable del Tratamiento o a quién este designe, podrán autorizar la salida de datos de carácter personal en soportes extraíbles de la organización.

Disposición final de soportes.

Reutilización:

Cuando un equipo deba ser reasignado a otro trabajador de la organización, por ejemplo, porque su usuario actual varía de función dentro de la empresa o bien deja de prestar servicios para la misma, el Responsable del Tratamiento, se encargará de solicitar la entrega y devolución cualquier dispositivo a través del cual puedan tratarse datos personales, incluso aquellos que otorguen el acceso físico a instalaciones y dependencias de la organización.

A tales fines, se procederá de la siguiente forma:

* Antes de reasignar el dispositivo o equipo en cuestión, se procederá a realizar copia de la información que contengan, en caso de ser necesario.
* Una vez realizada la copia de seguridad, se procederá a realizar un formato completo, de tal forma que no se mantengan usuarios ni claves.
* Realizado el formato completo y configurado el equipo para el nuevo usuario, se procederá a su entrega, previa firma el registro de entrega de dispositivo al trabajador.

**Disposición final:**

Se informa que la destrucción de la documentación, ya sea en soporte papel o digital, que se genera como consecuencia del desarrollo de las funciones inherentes al puesto de trabajo, sobre todo cuando se contenga datos personales, tiene una labor previa que si no se realiza correctamente puede derivar en un incumplimiento de la normativa de protección de datos.

Por lo expuesto, no pueden tirarse los documentos ni soportes, de ningún tipo, directamente a la basura, ni aunque se rompan en trozos; la disposición final de los mismos se realizará de la siguiente forma:

* Si se va a desechar el soporte, por ejemplo, un ordenador, portátil o móvil, discos duros, DVD’s, CD’s, memorias USB, cintas o cualquier otro tipo de dispositivo digital; por mal funcionamiento, antigüedad, inutilidad, etc., el empleado deberá ponerlos a disposición del Responsable del Tratamiento o de la persona designada por este a tal, para que dicha persona proceda a su desechado.
* Destruir los papeles que contengan información personal empleando las destructoras de papel debe ser en partículas habilitadas a tal fin, dentro de las instalaciones del responsable.

Procedimiento de notiﬁcación, gestión y respuesta ante las incidencias.

El procedimiento de notiﬁcación y gestión de incidencias consistente en violaciones de datos por parte de terceros, mediante acceso no consentido on-line o presencial, debe contener un registro en el que conste:

* El tipo de incidencia.
* El momento en que se ha producido.
* La persona que realiza la notificación.
* A quién se le comunica.
* Los efectos que se hubieran derivado de la misma.
* El sistema informático utilizado en caso de tratarse de gestión automatizada.

**POLITICAS DE DESECHADO Y REUTILIZACIÓN DE SOPORTES Y EQUIPOS**

La organización con el fin de garantizar la privacidad, confidencialidad y seguridad de los datos de carácter personal durante el proceso de destrucción, desechado o reasignación de soportes, evitando el acceso a la información contenida en los mismos o su recuperación posterior, establece las siguientes políticas generales de actuación.

Asimismo, el objetivo es dar cumplimiento al principio de responsabilidad proactiva establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

La razón por la que se debe realizar una destrucción confidencial tanto de la información obsoleta como de los soportes que la almacenan es evitar posibles brechas de seguridad, definidas éstas en el RGPD como una violación de seguridad de los datos en aquellos casos en los se ocasione “la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.”

Así pues, antes de eliminar o reutilizar un soporte que haya almacenado información personal o confidencial se deben aplicar los procedimientos establecidos en esta política para evitar la recuperación de la información una vez destruida.

La presente política resulta de aplicación a todos los puestos de trabajo, instalaciones y equipos ubicados dentro de las instalaciones de la Organización

Los usuarios de este documento es todo el personal de la Organización que traten datos de carácter personal o información confidencial.

Desechado

La destrucción de la documentación, ya sea en soporte papel o digital, que se genera en los distintos ámbitos de la empresa sobre todo cuando esta contenga datos personales, tiene una labor previa que si no se realiza correctamente puede derivar en un incumplimiento de la normativa de protección de datos vigente.

Por lo expuesto, no se tiran los documentos ni soportes de ningún tipo que contenga datos personales, directamente a la basura, ni aunque se rompan en trozos, debiendo proceder a la destrucción de los soporte de la siguiente forma:

* Los soportes, por ejemplo, un ordenador, portátil o móvil, discos duros, DVD’s, CD’s, memorias USB, cintas o cualquier otro tipo de dispositivo digital; antes de ser desechados por mal funcionamiento, antigüedad, inutilidad, se ponen a disposición del Responsable del Tratamiento o de la persona designada por este.
* La información contenida en papel, se desecha en las destructoras de papel habilitadas por la Organización dentro de las instalaciones del Responsable.

Reutilización

Cuando un equipo utilizado previamente por un empleado/socio/ voluntario se reasigna a otro miembro de la Organización, por ejemplo, como consecuencia de una movilidad funcional dentro de la empresa del primero o bien finalización del contrato laboral, despido o renuncia voluntaria de este, se establece el siguiente procedimiento de actuación.

* Antes de reasignar el dispositivo o equipo en cuestión a otro empleado, y siempre en caso de ser necesario, se realizan copias de la información contenida en el dispositivo reasignado.
* Una vez realizada la copia de seguridad, el dispositivo objeto de reasignación es formateado de forma completa empleando técnicas de formateo de nivel alto, de tal manera que no se mantengan usuarios ni claves asignadas con anterioridad.
* Realizado el formateo completo y configurado nuevamente el equipo para el nuevo empleado, se procederá a su entrega, previa firma el registro de entrega de dispositivo al personal.

La presente política debe ser conocida y estar accesible para todos los integrantes de la entidad, por lo cual se distribuirá la misma a través de los canales habilitados para ello dentro de la organización.

**POLÍTICA DE PANTALLA Y ESCRITORIOS LIMPIOS**

La organización establece la siguiente política de pantalla y escritorios limpios con la finalidad de evitar el acceso no autorizado a los documentos impresos y/o soportes que almacenen datos de carácter personal. Dando así cumplimientos al principio de responsabilidad proactiva establecidos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016.

La presente política resulta de aplicación a todos los puestos de trabajo, instalaciones y equipos ubicados dentro de las instalaciones de la Organización.

Los usuarios de este documento son todos los integrantes de la Organización (personal laboral, altos cargos y directivos.)

Escritorio Limpio

En el caso de que el personal laboral se ausente del puesto de trabajo, todos los documentos impresos, como también los soportes de almacenamiento de datos que contengan datos personales, deben ser retirados del escritorio o de otros lugares (impresoras, equipos de fax, fotocopiadoras, etc.) para evitar el acceso no autorizado a los mismos.

El puesto de trabajo debe estar limpio y ordenado.

El personal laboral solo podrá disponer únicamente de los activos que la empresa pone a su disposición.

Se prohíbe colocar sobre los escritores y mesas de trabajo, recipientes o envases cuyo cierre no sea hermético y que contengan líquidos, con el fin de evitar su vertido encima de los equipos informáticos y/o cualquier otro tipo de soporte que pueda verse afectado por el vertido.

Pantalla Limpia

La ubicación de los puestos de trabajo y la colocación de las pantallas dentro de la Entidad está organizada de tal forma que sólo la persona que utiliza la misma puede leer lo que se plasma en la pantalla, evitando miradas indiscretas.

En el caso de que el personal laboral se ausente del puesto de trabajo, deberá quitar toda la información sensible de la pantalla y bloquear el acceso a todos los sistemas para los cuales la persona tiene autorización.

En el caso de una ausencia corta (hasta 30 minutos), la política de pantalla limpia se deberá implementar finalizando la sesión en todos los sistemas o bloqueando la pantalla mediante el uso de la siguiente combinación de teclas:

*Botón Windows + L*

En el caso de una ausencia por un período más prolongado (superior a 30 minutos), la política de pantalla limpia se deberá implementar finalizando la sesión en todos los sistemas y apagando el ordenador.

La presente política debe ser conocida y estar accesible para todos los integrantes de la organización, por lo cual se distribuirá la misma a través de los canales habilitados para ello dentro de la organización.

ANEXOS

**ANEXO 1**

INFORME DE ACTIVOS INFORMÁTICOS DE LA ENTIDAD

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nº | Nombre | Estado | Descripción | Medio de Conservación | Responsable | Tipo | Disponibilidad | Confidencialidad | Seguridad | Valor asignado |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |