Política de Seguridad de la Información

1. Objetivo

El presente documento contiene la Política de Seguridad que **MEDIPERU S.A.** pone a disposición de todos sus trabajadores. El objetivo es proteger la calidad y seguridad de la información. Para ello se detallan una serie de políticas y procedimientos sobre las medidas técnicas y organizativas que puedan garantizar la adecuada gestión de la información y protección de los datos personales que gestiona como empresa, incluyendo los datos personales de los bancos de datos de titularidad de las empresas del Grupo Bupa.

2. Responsables

2.1. Es responsabilidad del jefe de cada área hacer cumplir la presente política.
2.2. Es responsabilidad del Jefe de Sistemas vigilar, actualizar y divulgar la presente política.
2.3. Es responsabilidad de todos los trabajadores cumplir los lineamientos descritos en la presente política.

3. Políticas y procedimientos

La Política de Medidas de Seguridad de los Recursos Informáticos está compuesta por las siguientes políticas y procedimientos:

3.1. Control de registros y accesos.-

- Gestión de accesos: Para impedir accesos no autorizados a los recursos informáticos de la empresa se deben establecer procedimientos para asignar derechos de acceso a los sistemas. Para ello se debe tomar en consideración la condición de los trabajadores que son usuarios de los sistemas en la empresa, desde su ingreso como trabajador y su cese, tomando especial consideración en los trabajadores que tienen accesos privilegiados. Los procedimientos deben considerar: (i) registro de trabajadores que serán los usuarios de los sistemas de la empresa; (ii) gestión de accesos privilegiados y revisión periódica de los mismos,; (iii) gestión de contraseñas; (iv) altas y bajas de las cuentas; (v) cancelación de accesos debido al cese de la relación laboral; (vii) modificación de los perfiles de los trabajadores, toda modificación debe ser revisada por el jefe inmediato y validada por el área de recursos humanos; (viii) conformidad de los trabajadores activos, lo que ayudará a llevar un control de la vigencia de los trabajadores que están activos en la empresa de manera periódica.

- Responsabilidad de los colaboradores: Los trabajadores que son usuarios de los sistemas de la empresa deben ser informados de sus responsabilidades y de que el éxito de las medidas de seguridad depende de su cooperación. Se debe capacitar a los trabajadores en los siguientes temas: (i) uso de contraseñas; y (ii) equipos desatendidos.

- Control de acceso a los recursos informáticos: Para acceder a los recursos informáticos de la empresa y para que los trabajadores no comprometan la seguridad de la información, se establecen mecanismos de identificación y autenticación.
- Control de acceso a los sistemas de la empresa: El acceso a los sistemas de la empresa debe ser controlado para evitar accesos no autorizados, incluyendo procedimientos de inicio de sesión seguros.

- Control de acceso a las aplicaciones: Se debe impedir el acceso a la información que se encuentre en aplicaciones y restringir el acceso a los trabajadores que estén autorizados.

- Monitoreo de uso de los sistemas: Los sistemas deben ser monitoreados para detectar actividades no autorizadas y reportar cualquier incidente de seguridad.

- Computación móvil y teletrabajo: Evaluar las medidas de seguridad que proporcionen un nivel de seguridad acorde a la sensibilidad de la información y potenciales riesgos.

- Control de acceso lógico: Los recursos electrónicos deben contar con un control de acceso específico.

- Acceso lógico restringido: El acceso a todos los recursos está limitado a aquellos trabajadores y/o sistemas que cuenten con la autorización necesaria. El acceso de cualquier colaborador o sistema sin autorización, faculta a la empresa a tomar las acciones y sanciones pertinentes.

- Derecho de admisión acceso lógico: Se podrá denegar o bloquear el acceso a cualquier colaborador o sistema en casos justificados y de manera unilateral.

- Lista de acceso lógico autorizado: El área técnica pondrá a disposición de quienes requieran la información para su trabajo, las listas de colaboradores, sistemas con acceso autorizado y tipo de control de acceso.

3.2. Registros de interacciones. -

- Generación de registros: Cada vez que los trabajadores interactúen con los datos lógicos, se mantiene un registro para fines de trazabilidad.

- Registros: Se deben mantener registros de los trabajadores con acceso al sistema y actividades más relevantes realizadas en el sistema.

- Procedimiento de disposición: Los registros serán almacenados por 90 días para finalidades de seguridad y una vez que estos ya no sean útiles se efectuará su destrucción.

3.3. Registro de incidencias. -

- Incidente de seguridad informática: Es todo evento adverso vinculado a la seguridad de los sistemas y recursos informáticos.

- Clasificaciones del incidente: Los incidentes se pueden clasificar en: (i) fallas en aplicativos o servicios críticos; (ii) código malicioso; (iii) accesos no autorizados o mal uso de los recursos informáticos; (iv) violación de la presente Política de Medidas de Seguridad de los Recursos Informáticos.
- Prevención de incidentes: El área de sistemas toma las medidas técnicas necesarias para prevenir que ocurran incidentes y es obligación de todos los trabajadores acatar las medidas de seguridad para evitar la ocurrencia de incidentes.

- Detección y reporte del incidente: Una vez detectado el incidente o la existencia de un potencial incidente, y si este no es detectado por el área de sistemas, el área del trabajador que detecte el incidente o la potencial existencia de un incidente debe informar de manera inmediata al área de sistemas.

- Análisis del incidente: Una vez ocurrido el incidente de seguridad informática, se debe analizar su gravedad, a efectos de ver cuál serían las posibles respuestas o soluciones.

- Respuesta del incidente o medida adoptada: El área de sistemas es el encargado de tomar las acciones o medidas pertinentes para dar respuesta al incidente.

- Registro del incidente: Cualquier incidente que ocurra debe ser registrado en el registro de incidentes que administrará el área de sistemas.

- Prevención de nuevos incidentes: El área de sistemas dictará las medidas de prevención necesarias para evitar la ocurrencia de nuevos incidentes.

3.4. Copias o reproducciones. -

- Generación de copias: La generación de copias o la reproducción de los documentos únicamente podrán ser realizadas bajo el control del personal autorizado.

- Destrucción de Copias: Se deben destruir o eliminar las copias o reproducciones que ya no se vayan a utilizar. Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.

3.5. Gestión y uso de contraseñas. -

- Bloqueo de Pantalla (Protector de Pantalla)**:** El trabajador es responsable de proteger su información debidamente, teniendo que activar el protector de pantalla del equipo asignado siempre que deje su posición de trabajo.

- Contraseña de equipo de cómputo**:** El trabajador es responsable de mantener su contraseña vigente y de no compartirla con ningún otro trabajador como medida de seguridad, si el trabajador comparte su contraseña la responsabilidad recae completamente sobre él. El área de sistemas ha planificado que cada cierto tiempo se solicite el cambio de la contraseña (entre 30 a 90 días) para todos los colaboradores. La contraseña debe contener al menos 8 dígitos y ser alfanumérica (mayúsculas, minúsculas y números) e incluir un carácter especial.

- Contraseña de equipo de comunicaciones (Celulares)**:** En los equipos de comunicaciones donde se tenga información de la empresa, necesariamente se deberá activar una contraseña para restringir el acceso al equipo, por ningún motivo se puede desactivar la contraseña.

3.6. Seguridad de los equipos. -

- Seguridad física de equipos de cómputo (Desktops y Laptops)**:** Todos los trabajadores son responsables de mantener la seguridad del equipo en el puesto de trabajo asignado. En caso de requerir desplazar el equipo por algún motivo, se deberá informar previamente al jefe del área.

- Antivirus**:** El área de sistemas es responsable de mantener actualizado y vigente el software antivirus instalado en todos los equipos de cómputo. De existir sospechas de mal funcionamiento a causa de virus, los trabajadores deben comunicarse de inmediato con área técnica.

- Dispositivos de almacenamiento externo o medios informáticos removibles**:** El uso de este tipo de medios de almacenamiento externo (cintas de respaldo, memorias USB, disco duro externo, entre otros) debe de ser autorizado por el jefe del área del trabajador que desea hacer su uso.

- Eliminación de la Información de los medios informáticos removibles**:** Cuando se requiera eliminar información en un medio informático removible se deben utilizar mecanismos seguros de eliminación que garanticen la destrucción total de la información.

3.7. Conservación, respaldo y recuperación de datos. -

- Ambientes donde se conservan recursos informáticos: Los ambientes donde se conservan recursos informáticos cuentan con las medidas de seguridad apropiadas.

- Respaldos: Se han implementado mecanismos de respaldo de seguridad, los cuales permiten verificar la integridad de los datos personales almacenados en el respaldo.

- Recuperación: Ante una interrupción o daño se ha previsto la recuperación de los datos personales, garantizando el retorno al estado en el que se encontraban al momento en que se produjo la interrupción o daño.

3.8. Almacenamiento y traslado de documentación no automatizada. -

- Almacenamiento de datos no automatizados: Los archivadores u otros elementos donde se almacene información no automatizada con datos personales, se encontrarán resguardados bajo llave. Los archivadores permanecerán cerrados mientras no se estén utilizando los datos personales que contiene.

- Traslado físico dentro de la empresa: Cuando se traslade documentación física que contenga datos personales dentro de la empresa, se tomarán medidas que impidan el acceso o manipulación de dicha información.

- Traslado físico fuera de la empresa: Cuando se traslade documentación física que contenga datos personales fuera de la empresa, esto sólo se podrá hacer con la autorización del jefe del área que maneje dicha información y se hará utilizando los medios de transporte y medidas necesarias que eviten su acceso no autorizado, pérdida o manipulación durante el tránsito hacia su destino.

3.9. Uso de correos electrónicos. -

- Retención de correos electrónicos**:** Todos los trabajadores tienen una cuenta de correo electrónico asignada para realizar sus labores, la cual tiene un límite en su capacidad de almacenamiento, esta medida se toma para no bajar el rendimiento en el envío y recepción de los correos para todos los trabajadores.

- Uso de correos electrónicos**:** Todos los trabajadores deben de tener conocimiento del uso debido de los correos electrónicos corporativos. Tener en cuenta los siguientes puntos: (i) los correos electrónicos institucionales o de la empresa no deben ser utilizados para el envío de mensajes personales; (ii) Los trabajadores no podrán utilizar el correo electrónico de la empresa para distribuir información de la empresa sin autorización del jefe del área donde laboran; (iii) El trabajador debe de tener el debido cuidado para que los correos electrónicos personales corporativos no se entiendan como comunicados oficiales de la empresa; (iv) Los trabajadores no pueden utilizar el correo electrónico de la empresa para transmitir “cadenas de

mensajes"; (v) Ningún correo electrónico debe ser enviado con la intención de ocultar o modificar el nombre del emisor; (vi) Se proveerá una cuenta de correo electrónico a los contratistas mediante una solicitud de seguridad aprobada; (vii) Los trabajadores son responsables de todo correo electrónico procedente de su cuenta; (viii) Cuando se envíen documentos con información sensible o confidencial a través de un correo electrónico, los trabajadores deberán enviar el documento protegido con una contraseña o clave de seguridad.

4. Incumplimiento

Es responsabilidad de todo trabajador hacer cumplir las disposiciones indicadas en la presente política. En caso sucediera un incumplimiento, el responsable del proceso debe informar al área de recursos humanos, que evaluará el tipo de medida disciplinaria a aplicar.