0. LISTA DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
0	2020-12-14	Implementación de la norma
1	2022-01-18	Actualización políticas contraseñas
2	2022-03-31	Actualización Logo
3	2023-09-06	Revisión y actualización

TABLA DE CONTENIDO

1. OBJETIVO

Definir los lineamientos que permitan proteger y garantizar la disponibilidad y confidencialidad de la información.

2. ALCANCE

Esta política abarca todo el proceso de creación, distribución, almacenamiento y destrucción de la información y es aplicable para todos los trabajadores de planta, trabajadores en misión, empresas usuarias, proveedores, contratistas y terceros de todos los procesos de Empleamos Temporales SAS. Adicionalmente, para las personas naturales o jurídicas, nacionales o extranjeras que sin tener relación laboral o contractual con Empleamos Temporales S.A.S, tengan acceso a sus instalaciones, servicios e información.

3. DEFINICIONES

- **Dato:** es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **Confidencialidad:** es la garantía de que la información será protegida para que no sea divulgada sin consentimiento.
- **Disponibilidad:** acceso y uso de la información de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Integridad:** propiedad de salvaguardar la exactitud y estado completo de los activos.
- **Activo de Información:** es todo aquello que en la entidad es considerado importante o de alta validez para la misma, ya que contiene información importante como son bases de datos, usuarios, contraseñas, etc.
- **Copias de respaldo:** es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Servidor:** Es una aplicación (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque a la información.
- **Vulnerabilidad:** Es una debilidad del sistema informático que puede ser utilizada para causar un daño.

- **Incidente de seguridad de la información:** un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque.
- **Carpetas Compartidas:** su contenido será accesible para todos los usuarios que pertenezcan a un mismo grupo de trabajo.
- **Mesa de Ayuda de Tecnología:** es un centro de atención a los usuarios en donde se prestan servicios para gestionar requerimientos relacionados con los servicios TIC's.
- **OneDrive:** Sitio para almacenamiento virtual en la nube de la información.
- **Software:** es todo programa o aplicación programado para realizar tareas específicas.
- **Hardware:** es la parte física de un ordenador o sistema informático.

4. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la información es la manifestación que realiza la alta Dirección de Empleamos Temporales SAS sobre la intención de proteger la información generada, la infraestructura tecnológica y activos de la información, del riesgo que se genere de los accesos otorgados a empleados y terceros, garantizando confidencialidad, integridad y disponibilidad.

Empleamos Temporales S.A.S asume la responsabilidad de proteger los activos de información comprometiéndose a:

- Todo el personal será informado y responsable de la seguridad de la información, según sea relevante para el desempeño de su trabajo.

- Se dispondrá de financiación para la gestión operativa de los controles relacionados con la seguridad de la información y en los procesos de gestión para su implantación y mantenimiento.

- En ninguna circunstancia se podrá divulgar la información clasificada como CONFIDENCIAL o RESERVADA a personas no autorizadas o en espacios públicos o privados. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual.

- Los riesgos en seguridad de la información serán objeto de seguimiento y se adoptarán medidas relevantes cuando sea necesario.

- Fomentar la toma de conciencia de los trabajadores sobre la importancia de la seguridad de la información.

- Capacitar a los trabajadores sobre el uso y la responsabilidad que tienen al acceder a la información.

- Se debe hacer buen uso de los dispositivos móviles que son asignados para el desempeño de las funciones laborales.

- De acuerdo a lo establecido en el Articulo10 del Decreto 1377 del 2013, el cual reglamenta la Ley 1581 de 2012 sobre Protección de datos Personales, EMPLEAMOS TEMPORALES S.A.S, solicita por medio de la firma de un Consentimiento Informado, la autorización de los trabajadores, titulares de los datos para el tratamiento de la información y acceso de la misma.

- Cada usuario es el único responsable y conocedor de sus contraseñas, debe mantener la confidencialidad de las mismas y asegurarse de no revelarlas a nadie ya que pueden generarse inconvenientes en el caso de que otra persona las conozca he intente hacer transacciones, modificaciones o destruya información importante que puede afectar el desarrollo de sus funciones y las de la empresa.

- No anotar y/o almacenar en lugares visibles las contraseñas de acceso a los sistemas.

- La longitud de la contraseña debe ser como mínimo de 12 caracteres, aunque se recomienda usar contraseñas más largas.

- La contraseña debe contener al menos 3 caracteres alfabéticos de los cuales serán, al menos, una letra mayúscula y dos minúsculas.

- • La contraseña debe contener al menos 2 caracteres numéricos

- La contraseña debe tener al menos un caracter especial (` ~! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /).

- La contraseña no podrá contener el nombre o apellido del usuario, ni el documento de identidad del mismo.

- No compartir la contraseña bajo ningún concepto con otras personas, aunque sean de su mismo entorno.

- Guardar la información de contraseñas en un lugar seguro

- No utilizar para generar la contraseña palabras o nombres comunes que puedan figurar en diccionarios.

- No se podrán utilizar las tres últimas contraseñas empleadas.

- Las contraseñas deben cambiarse con regularidad, si el sistema no obliga al cambio es responsabilidad del usuario realizar este cambio.

- Las contraseñas se debe cambiar cada 2 meses por medidas de seguridad.

- Limitar el acceso del personal a aquellas áreas que hayan sido restringidas por razones de seguridad.

- Garantizar que los proveedores de servicios tecnológicos instalen y administren software y sistemas operativos legales.

- La descarga o instalación de cualquier tipo de software por los usuarios debe estar debidamente aprobado.

- Cada empleado tiene la responsabilidad sobre el equipo de cómputo que le fue asignado para el desarrollo de sus funciones, por ello debe garantizar uso adecuado con el fin de mantener la correcta operatividad y la vida útil de los equipos.

- Los mantenimientos físicos y lógicos de los equipos deben ser realizado exclusivamente por las personas indicadas para esto.

- Los daños y dificultades con el hardware deben ser notificados a la mesa de ayuda del proveedor de inmediato para hacer las respectivas validaciones.

- El proveedor debe realizar periódicamente un respaldo de la información crítica y tener control de copias que permita conocer que información está respaldada y almacenada. Se deben probar los procedimientos de restauración, para asegurar que son efectivos y que pueden ser ejecutados en los tiempos establecidos.

- Las copias de respaldo deben tener el mismo nivel de protección de la información que poseen en su fuente original.

- Está prohibida la navegación en páginas de descargas de películas, series o programas.

- Se debe mantener instalado y actualizado el antivirus, en todos los equipos de cómputo, es responsabilidad del empleado verificar que el antivirus se encuentre activo y notificar cualquier novedad a tiempo.

- El correo electrónico se debe utilizar exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales, no se debe utilizar para otros fines.

- Dentro de los procesos de contratación de personal o de prestación de servicios, debe realizarse la verificación de antecedentes en Procuraduría, de acuerdo con la reglamentación.

- Las carpetas compartidas en OneDrive, serán administradas por las áreas encargadas, quienes velarán por el buen uso de la información y de las carpetas.

- Todos los dispositivos y unidades de almacenamiento removibles, tales como CD’s, dispositivos personales “USB”, discos duros externos, cámaras fotográficas, cámaras de video, celulares, entre otros, deben ser controlados desde su acceso a la red o los equipos físicos de Empleamos Temporales SAS.

- Evitar accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información de Empleamos Temporales SAS.

- Los visitantes deben permanecer acompañados de un Colaborador del Empleamos Temporales SAS, cuando se encuentren en las oficinas o áreas donde se maneje información.

- En caso de pérdida o robo de un equipo portátil se debe informar inmediatamente a la Dirección Administrativa, Dirección Comercial y de Servicios, Dirección Jurídica, Gerencia o Sistemas y se debe poner la denuncia ante las autoridades competentes.

- Todo el personal de Empleamos Temporales SAS debe bloquear la pantalla de su equipo de cómputo cuando no estén haciendo uso de este o que por cualquier motivo deba dejar su puesto de trabajo.

- Al imprimir documentos de carácter CONFIDENCIAL, estos deben ser retirados de la impresora inmediatamente. Así mismo, no se deben reutilizar papel que contenga información CONFIDENCIAL.

- Cuando un empleado se retire de la empresa voluntaria o involuntariamente, su jefe inmediato es el responsable de solicitar la cancelación de los usuarios y contraseñas asignados para el acceso a los sistemas de la empresa.

5. RESPONSABILIDADES

Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, o cuando se reciba un aviso de incidencia se procederá al bloqueo temporal o indefinido del usuario dependiendo de la gravedad y reiteración del incidente, siendo responsable el usuario titular.

6. APOYO DE LA ALTA DIRECCIÓN

Las Directivas de Empleamos Temporales SAS deben apoyar activamente la seguridad de la información dentro de la entidad y tener conocimiento de las responsabilidades para garantizar la integridad de esta, el compromiso se verá reflejado a través de:

- Se comprometen a velar por el cumplimiento de las políticas de seguridad de la información, para que los empleados a su cargo, las conozcan y apliquen.

- La alta dirección de Empleamos Temporales SAS apoyará y mantendrá cuando se requiera relaciones con empresas que presten asesoría especializada en seguridad de la información.

Luis Javier Tirado Muñoz
Representante Legal
Fecha: enero de 2022

Empleamos Temporales Responsabilidad y Compromiso	**CONTROL DE REGISTROS**	**Código**	PR-FO-047
		Fecha edición	2022-03-24
		Versión	1

FECHA	2023-09-06
CÓDIGO	AG-PR-006
NOMBRE	Política de seguridad de la información

PARA QUE SE USA: Registrar la política de seguridad de información de la organización

	DILIGENCIAR	**RECOLECTAR**	**ANALIZAR**
RESPONSABLE	Directora Administrativa/ Auxiliar de sistemas	Directora Administrativa/ Auxiliar de sistemas	Directora Administrativa/ Auxiliar de sistemas
LUGAR	Oficina/Virtual	Oficina/Virtual	Oficina/Virtual
FRECUENCIA	Cada que se realice una actualización		
AUTORIZADOS PARA SU CONSULTA: Direcciones de la empresa/Gerencia/Analista de Operaciones/Empleados/usuarios.			

ALMACENAMIENTO		
	ARCHIVO ACTIVO	**ARCHIVO INACTIVO**
LUGAR	\\OneDrive\Sistema Gestión de la Calidad\políticas y reglamentos	\\OneDrive\Sistema Gestión de la Calidad\políticas y reglamentos\versiones anteriores
TIEMPO	Indefinido	Indefinido
MEDIO	Digital	Digital
RESPONSABLE	Directora Administrativa/ Auxiliar de sistemas	Directora Administrativa/ Auxiliar de sistemas
CAUSA DE RETENCIÓN	Análisis	Consulta

DISPOSICIÓN FINAL	
ACCIÓN	**RESPONSABLE**
Almacenar en el archivo digital	Responsable de calidad