Política de Seguridad de la información

MANPOWER PROFESSIONAL LTDA.
MARCA EXPERIS

PO-30

Experis®
ManpowerGroup

1. OBJETIVO

Establecer los lineamientos definidos por la Dirección de Manpower Professional Ltda. para los servicios prestados a través de la Marca Experis en materia de seguridad de la información. Estos lineamientos buscan dar cumplimiento a los requisitos legales aplicables, así como responder a las necesidades y expectativas de las partes interesadas en los servicios de hunting, talento tecnológico y las soluciones tecnológicas y digitales. Para ello, también se tiene en cuenta la Política Global de Seguridad de la Información de ManpowerGroup como marco de referencia.

2. DEFINICIONES/GLOSARIO

1. **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
2. **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
3. **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
4. **Controles:** Medida que permite reducir o mitigar un riesgo. **Activo De Información:** conocimiento o información que tiene valor para la organización.
5. **Activo Crítico:** Son aquellos elementos o componentes que hacen parte de la infraestructura critica.
6. **Alta Dirección:** Persona o grupo de personas que dirigen y controlan al más alto nivel una entidad. Es la máxima autoridad en el sistema.
7. **Sistema de Gestión de seguridad de la información (SGSI):** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
8. **Amenaza**: causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
9. Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
10. **Autenticidad:** Busca asegurar la validez de la información en tiempo, forma y distribución. Así mismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
11. **Ciberseguridad**: Es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
12. **Cifrado:** Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
13. **Criptografía:** Práctica que consiste en proteger información mediante el uso de algoritmos codificados, hashes y firmas.
14. **Acceso Lógico**: restricción de acceso a los datos. Esto se logra mediante técnicas de ciberseguridad como id.
15. Resolución número 00500 de marzo 10 de 2021

3. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

Manpower Professional Ltda. a través de los servicios prestados por la marca Experis, entendiendo la importancia de sus activos de información para la prestación de sus servicios, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) buscando proteger la confidencialidad, integridad y disponibilidad de los activos de información en relación a los servicios de búsqueda, asignación y gestión o entrega de talento especializado en tecnologías de la información, así como la gestión de servicios y soluciones de proyectos tecnológicos, buscando establecer un marco de confianza en el ejercicio de su misión con los clientes, todo enmarcado en el estricto cumplimiento de las normas y legislación aplicable.

Asimismo, la organización reafirma su compromiso con la mejora continua del Sistema de Gestión de Seguridad de la Información, asegurando la revisión periódica de sus procesos, controles y objetivos, con el fin de garantizar su eficacia, adaptabilidad y alineación con las mejores prácticas y requisitos aplicables, contribuyendo a la protección integral de la información y a la satisfacción de las partes interesadas.

4. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Lograr que el 90% del personal completar y aprobar los programas de capacitación y campañas de concientización en seguridad de la información en los próximos 12 meses, utilizando plataformas internas y sesiones de capacitación presenciales y/o virtuales para garantizar cobertura.
- Gestionar y solucionar el 90% de los incidentes de seguridad registrados en los próximos 12 meses, mediante el reporte oportuno y seguimiento de casos, asegurando la implementación de acciones correctivas y preventivas para reducir la recurrencia.
- Alcanzar un nivel de eficacia mínimo del 80% en la verificación de la totalidad de los controles implementados del SGSI en un periodo de 12 meses, mediante la ejecución de revisiones sistemáticas a las matrices de riesgos de seguridad de la información, con el fin de identificar desviaciones, actualizar valoraciones y definir acciones de mejora

5. COMPROMISO DE LA ALTA DIRECCIÓN

La Alta Dirección se compromete a apoyar y liderar el establecimiento, implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI); así mismo, se compromete a revisar el avance de la implementación del SGSI de manera periódica y garantizará los recursos suficientes (tecnológicos, financieros y de talento humano) para implementar y mantener el sistema, incluyendo dentro de las decisiones estratégicas la seguridad de la información.

Adicionalmente, la Alta Dirección garantiza que la política de seguridad de la información y los objetivos de seguridad de la información estén establecidos y sean compatibles con la dirección estratégica de la organización; asegura la integración de los requisitos del SGSI en los procesos de la organización; comunica la importancia de una gestión eficaz de la seguridad de la información y del cumplimiento de los requisitos del SGSI; vela porque el sistema logre los resultados previstos;

dirige y apoya a las personas para que contribuyan a la eficacia del SGSI; promueve la mejora continua del sistema; y respalda a otros roles gerenciales relevantes para demostrar liderazgo en lo que respecta a sus áreas de responsabilidad.

6. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

El Sistema de Gestión de Seguridad de la Información (SGSI) de Manpower Professional Ltda., para la marca Experis Colombia, abarca todos los procesos, recursos, activos y actividades relacionados con la prestación de servicios de búsqueda, asignación, gestión y entrega de talento especializado en tecnologías de la información, así como la gestión de servicios y soluciones de proyectos tecnológicos.

El SGSI ha sido definido considerando el contexto interno y externo, los requisitos legales y regulatorios, las expectativas de las partes interesadas, y los riesgos asociados a la seguridad de la información. También se han considerado las interfaces y dependencias entre las actividades internas y las realizadas por terceros, las cuales se gestionan mediante acuerdos formales, controles específicos y mecanismos de supervisión, garantizando la confidencialidad, integridad y disponibilidad de la información en todo el ciclo de vida del servicio.

Este alcance aplica y centra sus operaciones desde Bogotá con los servicios, y desde Medellín, incluyendo las áreas organizacionales vinculadas, gestionando la seguridad de la información, el mantenimiento del SGSI y la administración del centro de datos, trabajando de forma articulada para asegurar el cumplimiento de los objetivos de seguridad de la información.

Los controles del Anexo A que aplican al SGSI han sido seleccionados y justificados en la Declaración de Aplicabilidad (SoA), conforme a los requisitos.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

Experis, define los roles y responsabilidades para la implementación y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados así:

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Alta Dirección / Dirección Experis y Gerente General	• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información (Recursos económicos, formación y recursos tecnológicos).
	• Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información.

PO-30. Política de Seguridad de la Información

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Dirección de Tecnología y transformación TI	• Implementar los controles de tipo tecnológico que apliquen para ayudar a mitigar los riesgos de seguridad de la información dentro de los procesos involucrados en la prestación de los servicios.
BDM (Business Development Manager)	• Implementar los controles de tipo tecnológico que apliquen para ayudar a mitigar los riesgos de seguridad de la información en la relación comercial con los clientes a través de las ofertas comerciales y los contratos de servicio.
Oficial de Seguridad del SGSI	• Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información y proponer las decisiones que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidas y aprobados por la entidad. • Apoyar en la generación de los lineamientos (Manuales, procedimientos y formatos) que permitan el establecimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información en la Entidad.
Coordinadores de Formación y desarrollo organizacional / Gestores de Servicios / Project Manager / Consultora Talento Humano	• Asegurar que los empleados staff y Staffing tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.
Coordinación del SG / Dirección de People & Culture	• Incluir la seguridad de la información, dentro de los planes de auditoría interna. • Apoyar en situaciones de posibles violaciones a las políticas de seguridad de la información.
Comunicaciones	• Apoyar en las labores de comunicación y sensibilización en seguridad de la información, para difundir la información en todos los niveles de la empresa.
Compras / Gestion de Riesgos / Administracion del SG/ Gestion de operaciones e infraestructura TI / Procesos operativos de Experis: Hunting – Outsourcing y soluciones tecnológicas y digitales	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas relacionados con la prestación de los servicios de Experis. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos en relación con la prestación de los servicios de Experis.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES (Definir los deberes respecto a la SEGURIDAD DE LA INFORMACIÓN)
Líderes de Proceso	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Todos los empleados	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos en relación con la seguridad de la información. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

Estas y otras responsabilidades se encuentran también adicionadas en los perfiles de cargo.

8. SANCIONES

Cualquier violación a las políticas de seguridad de la información de Manpower Professional Ltda. para los servicios prestados a través de la marca Experis debe ser sancionada de acuerdo con el proceso disciplinario indicado en el Reglamento Interno de Trabajo, así como a lo indicados en las normas, leyes y estatutos de la ley colombiana, la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.

Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de esta.

9. SEGUIMIENTO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN DEL SGSI

Se realizarán revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

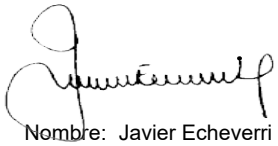
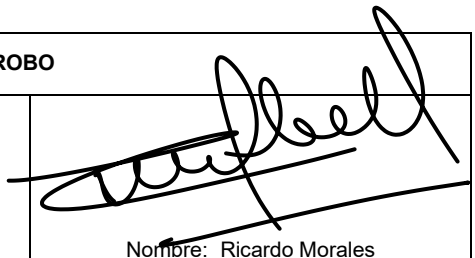
- Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
- Revisión de avance en la implementación del Sistema de Gestión de Seguridad de la Información.
- Revisión de avance de la Política de Seguridad de la información de acuerdo con lo solicitado por Sistema de Gestión de Seguridad de la Información.
- Revisión de los Riesgos de Seguridad de la Información y su tratamiento.

10. APROBACIÓN Y REVISIONES A LA POLÍTICA

Esta política será efectiva desde su aprobación por la Dirección de la Marca Experis y del Gerente General. La revisión de esta política se hará en las siguientes condiciones:

1. De forma anual, donde se deberá revisar la efectividad de la política y sus objetivos.
2. Si se dan cambios estructurales en la organización (restructuración de áreas o procesos).

3. Incidentes de seguridad de la información relacionados con la prestación de los servicios que requieran que la política cambie

APROBO	
 Nombre: Javier Echeverri Cargo: Country Manager	 Nombre: Ricardo Morales Cargo: Director de Experis Colombia

CONTROL DE CAMBIOS

Versión	Detalle	Fecha
1	Creación de la política	Octubre 1 de 2025
2	Se ajusta la política para incluir la mejora continua Se ajusta el compromiso de la dirección incluyendo los elementos del numeral 5.1 de la norma ISO 27001 Se ajustan todos los objetivos adaptados a la metodología Smart. Se ajustan las aprobaciones, incluyendo al Gerente General	Diciembre 17 de 2025