Política de seguridad de la información

CLASIFICACIÓN DE DOCUMENTOS	Interno
VERSIÓN	3.0
CON FECHA DE	14/07/2023
AUTOR DEL DOCUMENTO	Christina Georghiadou, directora de GRC
DUEÑO DEL DOCUMENTO	Marios Clark, vicepresidente senior de seguridad de la información y cumplimiento en ingeniería-liderazgo (CISO)

Revisión histórica

VERSIÓN	FECHA	AUTOR DE LA REVISIÓN	RESUMEN DE CAMBIOS
2.0	2/09/2022	Christina Georghiadou, directora de GRC	Se han realizado cambios para alinearse con la estructura ISO27001.
3.0	14/07/2023	Christina Georghiadou, directora de GRC	Cambios realizados en las siguientes secciones: 1) Áreas de la norma abordadas 2) Políticas temáticas específicas de seguridad de la información 3) Apéndice II

Distribución

EMPLEADOS
Todos los empleados

Aprobación

NOMBRE	POSICIÓN	FECHA
Marios Clark	Vicepresidente senior de seguridad de la información y cumplimiento	14/07/23

Contenido

Introducción

Este documento define la Política de Seguridad de la Información(el "**Política**") de las empresas del Grupo Jobandtalent (la "**Empresa**" o "**talento Job&Talent**") y reconoce la necesidad de garantizar que su negocio funcione sin problemas y sin interrupciones en beneficio de sus clientes y partes interesadas. Para proporcionar tal nivel de operación continua,Job&Talent ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI) en línea con el Estándar Internacional de Seguridad de la Información; ISO/IEC27001. Este estándar define los requisitos para un SGSI basado en las mejores prácticas reconocidas internacionalmente.

La operación del SGSI tiene muchos beneficios para el negocio, incluyendo:

- Protección de los flujos de ingresos y la rentabilidad de la empresa.
- Mantenimiento y mejora del valor para los stakeholders.
- Cumplimiento de requisitos legales y reglamentarios.

Objetivo

La Política de Seguridad de la Información es un documento obligatorio que compromete a la organización a garantizar una adecuada seguridad de la información.

Áreas de la norma abordadas

Este documento aborda las siguientes áreas de la norma ISO/IEC 27001:2022:

5.1	Políticas de seguridad de la información.
5.2	Funciones y responsabilidades de seguridad de la información

Alcance

Esta Política es aplicable a todos los empleados de Job&Talent y miembros del Consejo de Administración independientemente de la naturaleza de su relación con la Empresa, sin excepciones, independientemente de su ubicación geográfica y de las funciones que tengan encomendadas.

Asimismo, la Política también afecta a los socios o contratistas de Jobandtalent que, sin tener relación laboral o vínculo con la Empresa, hagan uso o tengan acceso a materiales, sistemas o dispositivos informáticos, de forma excepcional o periódica, propiedad de la Empresa.

Esta política se refiere a todos los sistemas y procesos Job&Talent.

Específicamente, esta Política se aplica a:

- Todas aquellas personas con acceso a los sistemas de información de Jobandtalent, incluidos el personal, visitantes y contratistas.
- Todos los datos o información mantenidos en formato impreso o electrónico por Jobandtalent, incluidos documentos, hojas de cálculo y otros datos, imágenes y videos en papel y electrónicos.
- Todos los sistemas conectados a las redes de Jobandtalent.
- Toda la información procesada por Jobandtalent de conformidad con sus actividades operativas, independientemente de si la información se procesa electrónicamente o en papel, incluidas todas las comunicaciones enviadas hacia o desde Jobandtalent.
- Todos los dispositivos informáticos personales y de propiedad de Jobandtalent, móviles o no, que se utilicen para acceder a los sistemas de información de Jobandtalent.
- Todos los terceros externos que prestan servicios a Jobandtalent con respecto a instalaciones de procesamiento de información y actividades comerciales.

Frecuencia de revisión

Esta política deberá actualizarse al menos anualmente o cuando ocurran cambios significativos en las operaciones de Job&Talent o en los estándares internacionales de seguridad.

Objetivos

- Mejorar continuamente la eficacia del SGSI
- Mejorar los procesos actuales para alinearlos con las buenas prácticas definidas en ISO/IEC 27001 y estándares relacionados.
- Mantener la certificación ISO/IEC 27001 de forma continua.
- Incrementar el nivel de proactividad en materia de seguridad de la información
- Hacer que los procesos y controles de seguridad de la información sean más mensurables para proporcionar una base sólida para decisiones informadas.
- Revisar las métricas relevantes trimestralmente.
- Obtener ideas para la mejora continua a través de reuniones periódicas y otras formas de comunicación con las partes interesadas.
- Revisar ideas de mejora en reuniones periódicas de gestión para priorizar y evaluar plazos y beneficios.

Se pueden obtener ideas de mejora de cualquier fuente, incluidos empleados, clientes, proveedores y/o evaluaciones de riesgos. Una vez identificados, se registrarán y evaluarán como parte de los procedimientos de revisión.

Principios de seguridad de la información

Jobandtalent ha adoptado los siguientes principios para respaldar esta Política:

- La información se protegerá de acuerdo con todas las políticas relevantes de Jobandtalent.
- Se mantendrá la integridad de la información.
- La información estará protegida contra el acceso no autorizado.
- Es responsabilidad de todas las personas a las que se les ha otorgado acceso a la información manejarla adecuadamente.

Cumplimiento de la política

Job&Talent medirá y verificará el cumplimiento de esta Política a través de varios métodos, incluidos, entre otros, informes de herramientas comerciales y auditorías internas y externas.

El incumplimiento de esta Política puede dar lugar a que se tomen medidas disciplinarias de acuerdo con la legislación local aplicable y, si corresponde, el Proceso Disciplinario de Empleados de Jobandtalent.

Las preguntas relacionadas con cualquier sección de esta Política deben dirigirse directamente al Director de GRC.

Excepciones

Puede surgir una situación que requiera otorgar una excepción a esta Política y la documentación de respaldo asociada.

Cualquier excepción se otorgará de manera controlada, incluida una justificación comercial/operativa detallada proporcionada por el jefe respectivo del departamento que solicita la excepción y la aprobación del Comité Directivo de Seguridad de la Información (o "**CISS**").

El Equipo de Seguridad mantendrá un registro de excepciones para el seguimiento, análisis y aprobación adecuados de las excepciones.

Las solicitudes de excepción a esta Política se presentarán al Director de GRC para su posterior evaluación. Se pueden otorgar excepciones a esta Política solo si puede existir una de las siguientes condiciones:

- Implementación de una solución con protección equivalente.
- Implementación de una solución con protección superior.
- Retiro inminente de un sistema heredado.
- Incapacidad para implementar la política debido a limitaciones del sistema o de la funcionalidad.

Roles, Responsabilidades y Autoridades

El Consejo de Administración ("la **Junta**") es en última instancia responsable del gobierno corporativo en su conjunto. La gestión y control de los riesgos de seguridad de la información es parte integral del gobierno corporativo. El Directorio delega explícitamente responsabilidades ejecutivas en materia de gobierno corporativo a los Directores Ejecutivos, liderados por el Co-**Director ejecutivo (co-directores ejecutivos)**.

El **Codirector ejecutivo** dar dirección estratégica general aprobando y exigiendo el Manual de Seguridad de la Información (SGSI) y delegar responsabilidades operativas para los asuntos de seguridad de la información al Comité **Directivo del SGSI (ISMS-SC)** presidido por el **Director de seguridad de la información (CISO).**

El Co director **ejecutivo** depende en gran medida del ISMS-SC para coordinar las actividades en todo Jobandtalent, garantizando que existan políticas adecuadas para respaldar los principios y axiomas de seguridad de jobandTalent. El director **ejecutivo** también confía en la retroalimentación del ISMS-SC, CISO, Director de GRC y auditores externos para garantizar que los principios, axiomas y políticas se cumplan en la práctica.

El Codirector **ejecutivo** demuestra su compromiso con la seguridad de la información al:

- Revisar y re-aprobar el SGSI.
- Aprobar el presupuesto de TI incluyendo un elemento específico destinado a la seguridad de la información.
- Recibir y actuar adecuadamente sobre los informes de gestión relativos a métricas de seguridad de la información, incidentes de seguridad, solicitudes de inversión,*etc.*.

El SGSI**-SC** es responsable de:

- Supervisión y dirección de la gestión de los aspectos físicos y lógicos de la seguridad, incluida la seguridad de la información;
- Coordinar y dirigir todo el marco de seguridad de Jobandtalent, incluidos los controles de seguridad de la información en todas las ubicaciones.
- Revisar periódicamente las declaraciones de la política de seguridad para garantizar la eficiencia y eficacia de la infraestructura de controles de seguridad de la información en su conjunto, recomendando mejoras cuando sea necesario;
- Identificar tendencias y cambios significativos en los riesgos de seguridad de la información de Jobandtalent y, cuando corresponda, proponer cambios en el marco de controles y/o políticas, por ejemplo, patrocinando importantes iniciativas estratégicas para mejorar la seguridad de la información;
- Revisar los incidentes críticos de seguridad y, cuando corresponda, recomendar mejoras estratégicas para abordar las causas fundamentales subyacentes;

El ISMS-SC delega algunas de sus responsabilidades (por ejemplo, al equipo de seguridad), pero sigue siendo responsable ante la junta directiva de la eficacia general de la seguridad de la información en todo Jobandtalent.

Diferentes ubicaciones dentro de Jobandtalent tienen Gerentes **de país locales (LCM)** que reportan al ISMS-SC. Los LSC son responsables de:

- Proporcionar la dirección estratégica, el apoyo y los recursos necesarios para gestionar todo tipo de problemas de seguridad local y así garantizar que los activos de información de Jobandtalent estén protegidos de forma adecuada y consistente;
- Coordinar y compartir información entre sí para garantizar la ejecución consistente de la política de seguridad de la información en todas las ubicaciones de Job and Talent;

- Identificando específicos Activos **de información significativos**, clasificándolos y nombrando propietarios de activos de información adecuados (**IAO**) para ellos;
- Recopilar métricas y otra información sobre la eficacia general de los controles de seguridad de la información en su ámbito de competencia e informar esto al ISMS-SC.

VP Sénior de Seguridad de la Información y Cumplimiento en Ingeniería- Liderazgo/ Director de seguridad (CISO) es responsable de:

- Presidir el ISMS-SC;
- Asumir el liderazgo en la gobernanza de la información en su conjunto y proporcionar la dirección estratégica general, el apoyo y la revisión necesarios para garantizar que los activos de información se identifiquen y protejan adecuadamente en todo Jobandtalent;
- Nombrar y gestionar los equipos de Seguridad y GRC.

El Director **de GRC**, que sustituye al CISO (si es necesario), es responsable de:

- Diseño, implementación y gestión del programa ISMS y GRC.
- Comunicar la estrategia y visión del equipo de seguridad.
- Proporcionar métricas basadas en evidencia y un marco de puntuación para medir el éxito del programa
- Definir estándares, procedimientos y lineamientos de seguridad de la información;
- Apoyar a los IAO y gerentes en la definición e implementación de controles, procesos y herramientas de apoyo para cumplir con el manual de políticas y gestionar los riesgos de seguridad de la información;
- Revisar y monitorear el cumplimiento de las declaraciones de políticas y contribuir a los procesos de Auditoría;
- Apoyar a las IAO en la investigación y remediación de violaciones de las políticas de seguridad de la información;
- Organizar una campaña de concientización sobre seguridad para el personal para mejorar la cultura de seguridad y desarrollar una amplia comprensión de los requisitos de ISO/IEC 27002.

Gerente En Jobandtalent somos responsables de:

- Implementación diaria de la política de seguridad de la información;
- Garantizar que se establezcan controles técnicos, físicos y de procedimiento adecuados de acuerdo con esta Política y que todos los empleados los apliquen y utilicen adecuadamente.
- Proporcionar la dirección, los recursos, el apoyo y la revisión necesarios para garantizar que los activos de información estén protegidos adecuadamente dentro de su área de responsabilidad;
- Informar al equipo de seguridad sobre violaciones de políticas reales o sospechadas (incidentes de seguridad de la información) que afecten sus activos; y
- Contribuir a las evaluaciones de cumplimiento organizadas por el Equipo de Seguridad.

Propietarios de activos de información (IAO) son administradores responsables de la protección de Activos de Información particulares. Las IAO son responsables de:

- Clasificación y protección adecuadas de los activos de información;
- Autorizar el acceso a los activos de información de acuerdo con la clasificación/necesidades del negocio;
- Garantizar la finalización oportuna de las revisiones periódicas del sistema/acceso a los datos; y
- Supervisar el cumplimiento de los requisitos de protección que afecten a sus bienes.

Todos los empleados de Jobandtalent son responsables de cumplir con las declaraciones de políticas enumeradas en este documento y cualquier otro principio de políticas específicas de un tema cuando sea relevante para sus trabajos. Son responsables de mantener la seguridad de toda la información que se les confía. Al ser contratado, como condición de empleo, cada trabajador se compromete a cumplir con las políticas de seguridad de la información de Jobandtalent.

La tabla RASCI, que se encuentra en el Apéndice I de esta Política, asocia roles en la organización con las secciones de ISO/IEC 27002.

Áreas de política de seguridad de la información

1.1 Seguridad de los recursos humanos

1.1.1 Antes del empleo

- Los empleados y contratistas, como parte de sus obligaciones contractuales, deberán comprender, aceptar y firmar los términos y condiciones (por ejemplo, como parte de un contrato) que también indicarán sus responsabilidades **de seguridad de la información**.
- **Las Verificaciones de antecedentes** se llevarán a cabo de conformidad con las leyes y reglamentos pertinentes y de forma proporcional a los requisitos del negocio y los riesgos percibidos.

1.1.2 Durante el empleo

- Los empleados y contratistas deberán conocer y cumplir sus responsabilidades **de seguridad de la información.**
- Los empleados deberán completar al menos una vez al año las capacitaciones obligatorias de concientización sobre seguridad.

- Habrá una comunicación formal y comunicada **Proceso Disciplinario** vigentes para tomar medidas contra los empleados que hayan cometido una violación de la seguridad de la información.

1.1.3 Terminación o cambio de empleo

- Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio se enfatizará al empleado o contratista y se harán cumplir, en la medida de lo posible.

1.2 Gestión de activos

- Un Inventario **actualizado** de los activos asociados con la información y las instalaciones de procesamiento de información se mantendrán para garantizar una protección eficaz de los activos basada en el riesgo.
- Todos los activos de información serán propiedad por el propietario del activo designado.
- Los activos serán regresados, o reasignados, tras la terminación del empleo, contrato o acuerdo.
- Un uso **aceptable** de activos deberá estar en vigor. Esto puede ser parte del Código de Conducta de la Empresa.

1.2.1 Dispositivos móviles y teletrabajo

- Se adoptarán medidas de seguridad para gestionar **los riesgos introducidos por el uso de dispositivos móviles.** y para proteger la información a la que se accede, procesa o almacena el usuario puntos **finales.**
- Solo a los dispositivos **autorizados** se le permitirá el acceso a la información y los sistemas de la empresa.
- Solo Software **autorizado** se permitirá su instalación y ejecución.

1.3 Clasificación de la información y manejo de medios.

La información se clasificará (en términos de requisitos legales, valor y criticidad), etiquetados y manejados según la Política de Clasificación de la Información. En línea con los niveles de clasificación,**la información se divulgará, tanto interna como externamente, según la estricta necesidad de saberlo.**

1.4 Control de acceso

- Deberes y áreas de responsabilidad en conflicto serán aisladas para reducir las oportunidades de modificación o uso indebido no autorizado o involuntario de los activos de la Compañía. Esto debería aplicarse en la medida de lo posible y practicable.**Siempre que sea difícil segregar, se deberán considerar otros controles como el seguimiento de las actividades, pistas de auditoría y supervisión de la gestión.**
- El acceso del usuario se definirá y otorgará según la necesidad de saber y según el principio **de privilegio mínimo.**
- **Los procedimientos de gestión de acceso** estarán vigentes para el registro, baja, revisión y ajuste de los derechos de acceso, para todos los usuarios. Esto incluye usuarios privilegiados, cuentas de sistemas y servicios, y cualquier entidad que pueda requerir acceso a los activos de información de la Compañía.
- Dichos procedimientos también abordarán requisitos **de inicio de sesión seguro y gestión de contraseñas** (por ejemplo, longitud, complejidad, antigüedad, reutilización y bloqueo de cuenta de la contraseña).
- **Acceso al código fuente** estará estrictamente restringido a las funciones apropiadas.

1.5 Criptografía

- **Uso adecuado y eficaz de la criptografía.** Se implementarán medidas para proteger la confidencialidad, autenticidad y/o integridad de los datos durante el procesamiento, en tránsito y durante el almacenamiento, incluidas las copias de seguridad.
- Formal Proceso **de gestión de claves** estará en su lugar.

1.6 Seguridad de las operaciones

- **Se establecerán responsabilidades y procedimientos para las operaciones informáticas.** y segregación de funciones implementada, cuando corresponda, para reducir el riesgo de uso incorrecto, negligente o deliberado del sistema.
- **Los procedimientos operativos deben estar documentados.** y puestos a disposición de todos los usuarios que los necesiten.
- **Procedimientos de gestión de cambios** Deberán existir procedimientos, instalaciones de procesamiento de información y sistemas que afecten a la seguridad de la información.
- Se **controlará el uso de los recursos.**, sintonizado y realizando proyecciones de los requisitos de capacidad futuros para garantizar el rendimiento requerido del sistema.
- **Los entornos de desarrollo, pruebas y operativos deben estar separados** para reducir los riesgos de acceso no autorizado o cambios en el entorno operativo.
- **Se establecerán controles contra el malware** para todos los sistemas que almacenan o procesan información de la Compañía, p.e. en servidores y estaciones de trabajo comúnmente afectados por malware/virus. Cualquier sistema que se considere que no

requiere dichos controles se mantendrá en una Lista **de excepciones**, aprobado formalmente y revisado periódicamente.

- **Copias de seguridad de la información.**, las imágenes del software y del sistema se tomarán y probarán periódicamente de **acuerdo con un procedimiento de respaldo acordado y documentado.**
- **Registros de eventos que registran las actividades del usuario.** (incluidos los administradores), se producirán excepciones, fallos y eventos de seguridad de la información, se mantendrán protegidos contra manipulaciones y accesos no autorizados y se revisarán periódicamente.
- **Parches y actualizaciones** se aplicarán a todo el software, sistemas operativos (estaciones de trabajo y servidores) y dispositivos de red, según la criticidad del parche. Estos se probarán en entornos que no sean de producción y se aprobarán antes de lanzarlos a producción.
- Relojes de todos los sistemas de procesamiento de información pertinentes se sincronizarán con una única fuente horaria de referencia.
- **Instalación de software en sistemas operativos.** será controlado.
- Documentado Estándares **de configuración segura** (por ejemplo, directrices de refuerzo, configuraciones de referencia) deberán existir para los sistemas de información que almacenen o procesen información del cliente.
- **Información sobre vulnerabilidades técnicas de los sistemas de información.** que se utilizan se obtendrán de manera oportuna, se evaluará la exposición de la Compañía a dichas vulnerabilidades y se tomarán las medidas apropiadas para abordar el riesgo asociado.
- Evaluaciones técnicas periódicas, al menos anuales, en forma de evaluaciones **de vulnerabilidad y/o pruebas de penetración** Se realizará para detectar vulnerabilidades de seguridad tanto para los sistemas internos como para los externos.
- Los requisitos de auditoría y las actividades que implican la verificación de sistemas operativos se planificarán y acordarán cuidadosamente para minimizar las interrupciones en los procesos comerciales.

1.7 Seguridad de las comunicaciones

- **Las redes serán gestionadas y controladas.** proteger la información en sistemas y aplicaciones, implementando controles de seguridad, niveles de servicio y segmentación en función de la criticidad de los activos de información,**Por ejemplo** como sigue:
    - Controles de aplicaciones que limitan el acceso, p.**Cortafuegos de aplicaciones web** (WAF);
    - **Firewalls de red o listas de acceso** que limitan las redes que pueden conectarse a redes y zonas que alojan datos de clientes;
    - **Zonas restringidas**, como VLAN o subredes para aislar zonas que almacenan datos de clientes
    - Listas específicas de "permisos" de clientes que pueden conectarse a subredes y VLAN que alojan datos de clientes
- **Controles de transferencia de información** Se establecerán medidas para proteger la transferencia de información a través de todo tipo de canales de comunicación.
- **Prevención de pérdida de datos (DLP)** Se establecerán controles para evitar la fuga de datos de los clientes.
- Se establecerán controles para prevenir y mitigar ataques **de denegación de servicio (DoS)**.
- **Sistemas de Detección y Prevención de Intrusos (IDS/IPS)** Deberán existir procedimientos sobre cómo se monitorean los eventos y las medidas tomadas cuando se alcanzan los umbrales de detección.
- **Autenticación multifactor** se utilizará para acceder a sistemas que almacenen, transmitan o procesen datos de clientes.

1.8 Adquisición, desarrollo y mantenimiento del sistema.

1.8.1 Aprobación de adquisición o desarrollo de un sistema

Se establecerá un proceso formal para la aprobación **de nuevos proyectos, en base a criterios o umbrales** (por ejemplo, el tamaño y la complejidad del sistema nuevo o modificado). Dicho proceso

puede incluir un análisis de viabilidad, revisión del alcance, recursos, funciones y responsabilidades, y gestión de cambios.

1.8.2 Seguridad de la información en la gestión de proyectos.

La seguridad de la información debe ser abordada **e integrada en la gestión de proyectos** para garantizar que los riesgos de seguridad de la información se identifiquen y aborden como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto independientemente de su naturaleza, p.e. un proyecto para un proceso de negocio central, tecnología y otros procesos de soporte.

1.8.3 Ciclo de vida de desarrollo de software (SDLC)

Se establecerá y aplicará a los desarrollos un ciclo de vida de desarrollo de software (SDLC) para el desarrollo de software y sistemas. Como mínimo, esto abordará lo siguiente:

- Los cambios en los sistemas dentro del ciclo de vida del desarrollo se controlarán mediante el uso de procedimientos **formales de control de cambios.**
- **Promoción de código a producción.** requerirá aprobación a través de un proceso formal de gestión de cambios.
- Uso de automatizado análisis **de código fuente** herramienta para detectar defectos de seguridad en el código antes de la producción.
- Cuando Plataformas **operativas** se cambian, las aplicaciones críticas para el negocio se revisarán y aprobarán para garantizar que no haya un impacto adverso en las operaciones o la seguridad de la empresa.
- **Principios para diseñar sistemas seguros.** deberán establecerse, documentarse, mantenerse y aplicarse a cualquier esfuerzo de implementación del sistema de información.
- Se utilizarán estándares de la industria para construir **seguridad** para el ciclo de vida de desarrollo de sistemas/software (SDLC).
- La Compañía establecerá y protegerá adecuadamente entornos **de desarrollo seguros** para los esfuerzos de desarrollo e integración de sistemas.
- La Compañía supervisará y vigilará la actividad de cualquier desarrollo **de sistemas subcontratados**, donde corresponda.
- Donde corresponda,**paquetes de software proporcionados por el proveedor** no se modificarán a menos que exista un proceso controlado y acordado con el proveedor.
- **Programas de pruebas de aceptación** y se establecerán criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.
- **Los datos de producción no pueden almacenarse**/transmitirse/procesarse en entornos que no sean de producción.

1.9 Relaciones con proveedores

- Todos los terceros (por ejemplo, proveedores, vendedores, prestadores de servicios) estarán cubiertos por un contrato o acuerdo de servicio que incluya requisitos **de privacidad, seguridad y confidencialidad.**
- Programa **de gestión de riesgos de terceros** Deberán implementarse medidas, que incluirán una revisión y validación, cuando sea posible, de la implementación del control de seguridad de la información antes de que los datos del cliente se expongan a un proveedor o se subcontratan procesos críticos.
- Terceros Será **reevaluado** periódicamente de acuerdo con la criticidad de la información empresarial, los sistemas y los procesos involucrados.

1.10 Gestión de incidentes de seguridad de la información.

- Responsabilidades y Se **establecerán procedimientos** para garantizar una respuesta rápida, eficaz y ordenada ante eventos o incidentes de seguridad de la información.
- Los empleados y contratistas que utilizan los sistemas y servicios de información de la Compañía deben informar **cualquier debilidad de seguridad de la información observada o sospechada** en sistemas o servicios.
- **Documentación** Se mantendrá información sobre incidentes/eventos (problemas, notificaciones, resultados, remediación y medidas preventivas).

- Procedimientos para la identificación**, recopilación, adquisición y conservación de información**, que puede servir como prueba.

1.11 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.

- Los procesos, procedimientos y controles para asegurar el nivel requerido de continuidad durante una situación adversa se establecerán a través de un acuerdo formal.**Plan de Continuidad del Negocio (BCP)**.
- Las instalaciones de procesamiento de información se implementarán con redundancia suficiente para cumplir con los requisitos de disponibilidad.
- Plan **de Recuperación de Desastres (DRP)** Se establecerán medidas para garantizar una recuperación efectiva.
- Los Planes de Continuidad del Negocio y Recuperación de Desastres deberán ser probado **periódicamente**, al menos anualmente.

1.12 Cumplimiento

1.12.1 Cumplimiento de requisitos legales y contractuales

- Todo relevante requisitos **legislativos, reglamentarios y contractuales se** identificará, documentará y mantendrá actualizado el enfoque para cumplir estos requisitos.
- Se implementarán procedimientos apropiados para garantizar el cumplimiento de los requisitos legislativos, reglamentarios y contractuales relacionados con derechos **de propiedad intelectual y uso de productos de software propietarios.**
- **Los registros estarán protegidos** contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos reglamentarios, contractuales y comerciales.
- **La privacidad y protección de datos personales** se garantizará según lo exige la legislación y la reglamentación pertinentes.
- **Los controles criptográficos** se utilizarán de conformidad con todos los acuerdos, leyes y reglamentos pertinentes.

1.12.2 Revisiones de seguridad de la información

- El enfoque de la Compañía para gestionar la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) serán revisados **de forma independiente a intervalos planificados o cuando se producen cambios significativos.**
- **Departamento / Función / Líderes de equipo** se asegurará de que los procedimientos operativos relevantes dentro de su área de responsabilidad estén definidos, en línea con esta Política y cualquier otra política, estándar y directriz de apoyo.
- **Sistemas de información** se revisarán periódicamente para verificar el cumplimiento de las políticas y estándares de seguridad de la información de la Compañía.

Políticas temáticas específicas de seguridad de la información

Esta Política consta de una amplia variedad de medidas de seguridad de la información. políticas temáticas específicas que se describen en detalle en un conjunto completo de documentación de políticas que acompaña a esta política general de seguridad de la información.

La siguiente tabla muestra las políticas individuales dentro del conjunto de documentación y resúmenes.ConEs el contenido de cada política y el público objetivo de partes interesadas:

Título de la póliza	**Objetivo**	**Público objetivo**
Política de control de acceso	Limitar el acceso a la información y a los sistemas, redes e instalaciones de procesamiento de información a partes autorizadas de acuerdo con los objetivos comerciales.	Empleados involucrados en la configuración y gestión del control de acceso.
Política de uso aceptable de la información	Establecer las responsabilidades de los empleados por el uso de la información y los activos.	Todos los empleados
Política de Clasificación de Información	Definir una forma de clasificar la información para que se le pueda aplicar el nivel correcto de protección.	Todos los empleados
Política de gestión de activos	Establecer las reglas sobre cómo se gestionan los activos en su ciclo de vida desde una perspectiva de seguridad de la información.	Todos los empleados
Política de seguridad de proveedores de nube	Garantizar la debida diligencia, instalación, gestión y eliminación de servicios de computación en la nube.	Empleados involucrados en la adquisición y gestión de servicios en la nube.
Política de Teletrabajo y Gestión de Dispositivos Móviles	Establecer los principios según los cuales los empleados deberán trabajar desde un lugar de teletrabajo. Establecer los principios según los cuales los empleados deberán utilizar dispositivos personales para acceder a los sistemas y datos corporativos.	Todos los empleados
Política criptográfica	Garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.	Empleados involucrados en la configuración y gestión del uso de tecnologías y técnicas criptográficas.

Política de seguridad de las comunicaciones	Garantizar que se implementarán mejores prácticas de seguridad en las redes de comunicación.	Empleados responsables del diseño, implementación y gestión de redes de comunicación.
Política de Recursos Humanos	Garantizar que los empleados y contratistas cumplan con los requisitos de seguridad, comprendan sus responsabilidades y sean adecuados para sus funciones.	Empleados responsables de asuntos de RRHH y Seguridad/Concienciación/formación
Política de gestión de incidentes de seguridad	Garantizar que los incidentes de seguridad sean correctamente identificados, registrados, analizados y contaminados.	Todos los empleados
Política de seguridad de operaciones	Garantizar el correcto y seguro funcionamiento de los sistemas e instalaciones de procesamiento de la información.	Todos los empleados involucrados en temas de seguridad de las operaciones.
Política de continuidad del negocio	Garantizar que al menos la operación crítica del negocio seguirá funcionando en caso de un incidente.	Empleados responsables de diseñar sistemas y gestionar servicios de continuidad del negocio.
Política de seguridad física	Para evitar el acceso físico no autorizado o daños a la información de la organización y a las instalaciones de procesamiento de información.	Todos los empleados
Política de gestión de riesgos	Definir el proceso de evaluación y gestión de los riesgos de seguridad de la información de Jobandtalent. con el fin de alcanzar los objetivos de negocio y de seguridad de la información de la Compañía.	Todos los empleados
Política de seguridad de la información para las relaciones con proveedores	Para garantizar la protección de los datos y activos de la organización que se comparten con los proveedores, son accesibles a ellos o son administrados por ellos, incluidos terceros u organizaciones de terceros, como proveedores de servicios, vendedores y clientes, y para mantener un nivel acordado de seguridad de la información y prestación de servicios de acuerdo con los acuerdos con los proveedores.	Empleados involucrados en el establecimiento y gestión de relaciones con proveedores.
Política de cumplimiento	Garantizar que las obligaciones de cumplimiento se documenten formalmente y se hagan cumplir a través de la organización.	Todos los empleados involucrados en los aspectos de cumplimiento del SGSI.

Política de gestión de excepciones	Determinar el procedimiento para otorgar exenciones a los Requisitos de Seguridad de la Información de la empresa.	Todos los empleados
Política de desarrollo seguro	El propósito de este documento es definir reglas básicas para el desarrollo seguro de software y sistemas.	Todos los empleados que realizan actividades de desarrollo.
Política de inteligencia artificial	Esta política tiene como objetivo proporcionar pautas específicas para garantizar la confidencialidad, integridad y disponibilidad de información confidencial al interactuar con herramientas de inteligencia artificial.	Todos los empleados cuyas acciones puedan exponer los sistemas o datos del JT a herramientas de IA generativa.
Política de Sensibilización y Formación	Garantizar que todos los empleados de la organización y, cuando corresponda, los contratistas reciban educación y capacitación adecuadas y actualizaciones periódicas sobre las políticas y procedimientos de la organización, según sea relevante para su función laboral.	Empleados de RR.HH. y equipo de seguridad

Apéndice I

Los roles se identifican como R, A, S, C o I, es decir:
Responsable (R) , es decir, esta función tiene la responsabilidad principal de realizar las actividades de esta sección.
Rendición de cuentas (A), es decir, este rol será llamado a rendir cuentas si los riesgos se materializan (generalmente porque fallan los controles preventivos).
Soporte (S) apoyo, es decir, esta función ayuda activamente con el diseño, implementación o gestión de las actividades de esta sección.
Consultado (C) Consultado, es decir, se trata de una función de no intervención, que ofrece orientación y dirección a quienes participan más activamente.
Informado (I), es decir, este rol tiene interés en el estado de los riesgos en esta sección y debe mantenerse en contacto con la situación.

Para conocer la asignación de controles a la norma ISO27001:2022, consulte el Apéndice II.

Sección de ISO/IEC 27002:2013 R = Responsable A = Responsable S = Solidario C = Consultado I = Informado		Propietarios de activos de información	Empleados	Coordinador ejecutivos	Vicepresidente Ingeniería	Comité Dirección ejecutivo de SI	CISO/Director de GRC	Equipo de seguridad	Jefe de Recursos Humanos	Jefe de Adquisiciones	Jefe de Asuntos Legales y Cumplimiento	Jefe de finanzas	Vicepresidente de la mesa de ayuda de TI	CTO	
5 Políticas de seguridad de la información															
5.1.1	**Políticas de seguridad de la información.**	C	I	C	A	S	r	S	C	S	C	C	C	S	C

5.1.2	Revisión de las políticas de seguridad de la información.	C		S	A	r	S	C	S	S	S	S	C	S	S
6 Organización de la seguridad de la información																		
6.1.1	Funciones y responsabilidades de seguridad de la información	A	I		r	S	C		C		C			C	C
6.1.2	Segregación de deberes	A	I		C	r	C							C	
6.1.3	Contacto con autoridades	A			C	S	S				r				
6.1.4	Contacto con grupos de intereses especiales	A			C	C	r				S			S	
6.1.5	Seguridad de la información en la gestión de proyectos.	A			C	r	S							S	
6.2.1	Política de dispositivos móviles	A	I		C	r	S	C						C	
6.2.2	Teletrabajo	A	I		r	S	C	C						C	
7 Seguridad de los recursos humanos																		
7.1.1	Poner en pantalla	A				S			r						
7.1.2	Términos y condiciones de empleo	A	I			S			S		r				
7.2.1	Responsabilidades de gestión	A	I		r	S			S						
7.2.2	Concientización, educación y capacitación sobre seguridad de la información.	A	I		S	r			S		C				
7.2.3	Proceso Disciplinario	A	I		S				r						
7.3.1	Terminación o cambio de responsabilidades laborales.	A	I			S			S		r			S	
8 Gestión de activos																		
8.1.1	Inventario de activos	A				S				r				C	
8.1.2	Propiedad de activos	A			r	S						S	S	C	
8.1.3	Uso aceptable de los activos	A	I			r	S	C	S	C			S		
8.1.4	Devolución de activos	A	I		r	C			S	S		C	S	S	
8.2.1	Clasificación de la información	A	I		S	r	C								
8.2.2	Etiquetado de información	A	I			S	r		C	C	C	C	S	S	
8.2.3	Manejo de activos	A	I			C	S					C	S	r	
8.3.1	Gestión de medios extraíbles.	A	I			S	S	C					S	r	
8.3.2	Eliminación de medios	A	I			S						C		r	
8.3.3	Transferencia de medios físicos	A	I			S	C	C						r	
9 control de acceso																		
9.1.1	Política de control de acceso	A			S	r	S	S	C	C				S	
9.1.2	Política de uso de servicios de red	A	I			S	C	S						r	
9.2.1	Alta y baja de usuario	A				S	C		r					S	
9.2.2	Aprovisionamiento de acceso de usuarios	A				S	C		r					S	
9.2.3	Gestión de privilegios	A				S								r	
9.2.4	Gestión de información secreta de autenticación de usuarios.	A				S	C	C						r	
9.2.5	Revisión de los derechos de acceso de los usuarios.	A			C	S	r	S	C					S	
9.2.6	Eliminación o ajuste de derechos de acceso.	A				S	S	C						r	
9.3.1	Uso de información de autenticación secreta	A	I			S		S						r	
9.4.1	Restricción de acceso a la información	A	I			S	C							r	

9.4.2	Procedimientos de inicio de sesión seguros	A				S	C								r			
9.4.3	Sistema de gestión de contraseñas	A				S	C	S							r			
9.4.4	Uso de programas de utilidad privilegiados.	A	I			S	C	S							r			
9.4.5	Control de acceso al código fuente del programa.	A	I			S	C	S							r			
10 criptografía																		
10.1.1	Política sobre el uso de controles criptográficos	A	I			S	r								S			
10.1.2	Gestión de claves	A				S	r								S			
11 Seguridad física y ambiental																		
11.1.1	Perímetro de seguridad física	A	I			S	C							r	C			
11.1.2	Controles de entrada física	A	I			S	C							r	C			
11.1.3	Seguridad de oficinas, habitaciones e instalaciones.	A	I			S	C							r	C			
11.1.4	Protección contra amenazas externas y ambientales.	A	I			S	C							r	C			
11.1.5	Trabajar en áreas seguras	A	I			S	C							r				
11.1.6	Zonas de entrega y carga	A	I			S	C							r				
11.2.1	Ubicación y protección de equipos.	A	I			S	C							r				
11.2.2	Servicios públicos de apoyo	A				S	C							r	C			
11.2.3	Seguridad del cableado	A				S	C							S	r			
11.2.4	Mantenimiento de equipo	A				S	C							r				
11.2.5	Eliminación de activos	A	I			S	C							r				
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	A	I			S	C							C	r			
11.2.7	Eliminación segura o reutilización del equipo	A	I			S	C							S	r			
11.2.8	Equipo de usuario desatendido	A	I			S	C							S	r			
11.2.9	Política de escritorio despejado y pantalla despejada	A	I			S	C							S	r			
12 Seguridad de las operaciones																		
12.1.1	Procedimientos operativos documentados	A					C	S							r			
12.1.2	Gestión del cambio	A	I		S	r	S			S					S	C		
12.1.3	Gestión de capacidad	A			S	r				S				C	S	C		
12.1.4	Separación de entornos de desarrollo, pruebas y operativos.	A			S	r	C	S							S			
12.2.1	Controles contra malware	A			S		C	S		C					r	C		
12.3.1	Copia de seguridad de la información	A			r	S	C			S					S			
12.4.1	El registro de eventos	A			S	S	C	S		S					r			
12.4.2	Protección de la información de registro	A			S	S	r	C		S					S			
12.4.3	Registros de administrador y operador	A				S	r	S							S			
12.4.4	Sincronización del reloj	A					C	S							r			
12.5.1	Instalación de software en sistemas operativos.	A	I			S	C			C					r			
12.6.1	Gestión de vulnerabilidades técnicas.	A				S	S	S							r			
12.6.2	Restricciones en la instalación de software	A	I			S	S	S							r			
12.7.1	Controles de auditoría de sistemas de información.	A			S	S	r	S							S	C		
13 Seguridad de las comunicaciones																		
13.1.1	Controles de red	A				S	C	S							r			

13.1.2	Seguridad de los servicios de red.	A				S	C							r		
13.1.3	Segregación en redes	A				S	C							r	S	
13.2.1	Políticas y procedimientos de transferencia de información.	A	I			S	r							S		
13.2.2	Acuerdos sobre transferencia de información.	A			S	r	S							S		
13.2.3	mensajería electrónica	A	I		S	S	C				C			r		
13.2.4	Acuerdos de confidencialidad o no divulgación	A			S	S	S		S		r	S		S		
14 Adquisición, desarrollo y mantenimiento del sistema																
14.1.1	Análisis y especificación de requisitos de seguridad.	A			C	S	r			C				C	C	
14.1.2	Protección de servicios de aplicaciones en redes públicas	A			C	r	S	S						S	C	
14.1.3	Protección de transacciones de servicios de aplicaciones	A				S	C	S						r		
14.2.1	Política de desarrollo seguro	A			C	S	S							S	r	
14.2.2	Procedimientos de control de cambios	A			C	S	r			C				S	C	
14.2.3	Revisión técnica de aplicaciones tras cambios de plataforma operativa	A				S	r							S		
14.2.4	Restricciones sobre cambios en paquetes de software	A				S	S	S						r	C	
14.2.5	Procedimientos de desarrollo del sistema.	A				r	S							S	S	
14.2.6	Entorno de desarrollo seguro	A				S	S							S	r	
14.2.7	Desarrollo subcontratado	A				S	S	C						S	r	
14.2.8	Pruebas de seguridad del sistema	A				S	r	S						S	S	
14.2.9	Pruebas de aceptación del sistema	A	C			S	S							S	r	
14.3.1	Protección de datos de prueba	A				r	S	S						S	S	
15 Relaciones con proveedores																
15.1.1	Política de seguridad de la información para las relaciones con proveedores	A			C	r	S									
15.1.2	Abordar la seguridad en los acuerdos con proveedores	A				S	r				S			S		
15.1.3	Cadena de suministro de tecnologías de la información y las comunicaciones	A				S	r							S		
15.2.1	Seguimiento y revisión de servicios de proveedores.	A					S	C						r		
15.2.2	Gestión de cambios en los servicios de los proveedores.	A				S	S							r		
16 Gestión de incidentes de seguridad de la información																
16.1.1	Responsabilidades y procedimientos	A				r	S		S		C		S	S		
16.1.2	Informar eventos de seguridad de la información	A	I			S	r	S					S	S		
16.1.3	Informar debilidades de seguridad de la información	A	I			S	r	S					S	S		
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información.	A				r	S	S			C		S	S		
16.1.5	Respuesta a incidentes de seguridad de la información	A				S	r	S			C		S	S		
16.1.6	Aprender de los incidentes de seguridad de la información	A				r	S	C	C			C	C	C	C	
16.1.7	Recopilación de pruebas	A					r	S			C		S	S		

17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio																
17.1.1	**Planificación de la continuidad de la seguridad de la información.**	A				S	r							S	S	
17.1.2	**Implementación de la continuidad de la seguridad de la información.**	A			S	S	r							S	S	
17.1.3	**Verificar, revisar y evaluar la continuidad de la seguridad de la información.**	A					r	S						S	S	
17.2.1	**Disponibilidad de instalaciones de procesamiento de información.**	A			S	S	S							r	S	
18 Cumplimiento																
18.1.1	**Identificación de la legislación aplicable y requisitos contractuales.**	A	I	r	S	S	S				S			S	S	
18.1.2	**Derechos de propiedad intelectual (DPI)**	A	I	C	r	S	S				C				S	
18.1.3	**Protección de registros**	A	I	r	S	S	S								S	
18.1.4	**Privacidad y protección de la información personal**	A	I	C	S	S					r				S	
18.1.5	**Regulación de controles criptográficos**	A				r					C				S	
18.2.1	**Revisión independiente de la seguridad de la información.**	A			r	S									C	
18.2.2	**Cumplimiento de políticas y estándares de seguridad.**	A	I		S	r					C				S	
18.2.3	**Inspección de cumplimiento técnico**	A			S	r					C				S	

Apéndice II

ISO 27001:2013		Mapa	ISO 27001:2022	
ID de control	Nombre del control		ID de control	Nombre del control
5.1.1	Políticas de Seguridad de la Información	→	5.1	Políticas de seguridad de la información.
5.1.2	Revisión de las Políticas de Seguridad de la Información	→	5.1	Políticas de seguridad de la información.
6.1.1	Funciones y responsabilidades de seguridad de la información	→	5.2	Funciones y responsabilidades de seguridad de la información
6.1.2	Segregación de deberes	→	5.3	Segregación de deberes
6.1.3	Contacto con Autoridades	→	5.5	Contacto con autoridades
6.1.4	Contacto con Grupos de Interés Especial	→	5.6	Contacto con grupos de intereses especiales
6.1.5	Seguridad de la información en la gestión de proyectos	→	5.8	Seguridad de la información en la gestión de proyectos.
6.2.1	Política de dispositivos móviles	→	8.1	Dispositivos terminales de usuario
6.2.2	Teletrabajo	→	6.7	Trabajo remoto
7.1.1	Poner en pantalla	→	6.1	Poner en pantalla
7.1.2	Términos y condiciones de empleo	→	6.2	Términos y condiciones de empleo
7.2.1	Responsabilidades de gestión	→	5.4	Responsabilidades de gestión
7.2.2	Concientización, educación y capacitación sobre seguridad de la información	→	6.3	Concientización, educación y capacitación sobre seguridad de la información.
7.2.3	Proceso Disciplinario	→	6.4	Proceso Disciplinario
7.3.1	Terminación o cambio de responsabilidades laborales	→	6.5	Responsabilidades tras el despido o cambio de empleo
8.1.1	Inventario de Activos	→	5.9	Inventario de información y otros activos asociados
8.1.2	Propiedad de los activos	→	5.9	Inventario de información y otros activos asociados
8.1.3	Uso Aceptable de los Activos	→	5.10	Uso aceptable de la información y otros activos asociados
8.1.4	Devolución de Activos	→	5.11	Devolución de activos
8.2.1	Clasificación de la información	→	5.12	Clasificación de la información
8.2.2	Etiquetado de información	→	5.13	Etiquetado de información
8.2.3	Manejo de Activos	→	5.10	Uso aceptable de la información y otros activos asociados
8.3.1	Gestión de medios extraíbles	→	7.10	Medios de almacenamiento
8.3.2	Eliminación de medios	→	7.10	Medios de almacenamiento
8.3.3	Transferencia de medios físicos	→	7.10	Medios de almacenamiento
9.1.1	Política de control de acceso	→	5.15	Control de acceso
9.1.2	Acceso a Redes y Servicios de Red	→	5.15	Control de acceso
9.2.1	Alta y Baja de Usuario	→	5.16	Gestión de identidad
9.2.2	Aprovisionamiento de acceso de usuario	→	5.18	Derechos de acceso

9.2.3	Gestión de Derechos de Acceso Privilegiado	→	8.2	Derechos de acceso privilegiados
9.2.4	Gestión de información secreta de autenticación de usuarios	→	5.17	Información de autenticación
9.2.5	Revisión de los derechos de acceso de los usuarios	→	5.18	Derechos de acceso
9.2.6	Eliminación o ajuste de derechos de acceso	→	5.18	Derechos de acceso
9.3.1	Uso de información de autenticación secreta	→	5.17	Información de autenticación
9.4.1	Restricción de acceso a la información	→	8.3	Restricción de acceso a la información
9.4.2	Procedimientos de inicio de sesión seguro	→	8.5	Autenticación segura
9.4.3	Sistema de gestión de contraseñas	→	5.17	Información de autenticación
9.4.4	Uso de programas de utilidad privilegiados	→	8.18	Uso de programas de utilidad privilegiados.
9.4.5	Control de acceso al código fuente del programa	→	8.4	Acceso al código fuente
10.1.1	Política sobre el uso de controles criptográficos	→	8.24	Uso de criptografía
10.1.2	Gestión de claves	→	8.24	Uso de criptografía
11.1.1	Perímetro de seguridad física	→	7.1	Perímetros de seguridad física
11.1.2	Controles de entrada física	→	7.2	Entrada física
11.1.3	Seguridad de oficinas, habitaciones e instalaciones	→	7.3	Seguridad de oficinas, habitaciones e instalaciones.
11.1.4	Protección contra amenazas externas y ambientales	→	7.5	Protección contra amenazas físicas y ambientales.
11.1.5	Trabajar en áreas seguras	→	7.6	Trabajar en áreas seguras
11.1.6	Áreas de entrega y carga	→	7.1	Perímetros de seguridad física
11.2.1	Ubicación y protección de equipos	→	7.8	Ubicación y protección de equipos.
11.2.2	Servicios públicos de apoyo	→	7.11	Servicios públicos de apoyo
11.2.3	Seguridad del cableado	→	7.12	Seguridad del cableado
11.2.4	Mantenimiento de equipo	→	7.13	Mantenimiento de equipo
11.2.5	Eliminación de activos	→	7.1	Perímetros de seguridad física
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	→	7.9	Seguridad de los activos fuera de las instalaciones
11.2.7	Eliminación segura o reutilización del equipo	→	7.14	Eliminación segura o reutilización del equipo
11.2.8	Equipo de usuario desatendido	→	8.1	Dispositivos terminales de usuario
11.2.9	Política de escritorio limpio y pantalla limpia	→	7.7	Escritorio claro y pantalla clara
12.1.1	Procedimientos operativos documentados	→	5.37	Procedimientos operativos documentados
12.1.2	Gestión del cambio	→	8.32	Gestión del cambio
12.1.3	Gestión de capacidad	→	8.6	Gestión de capacidad
12.1.4	Separación de entornos operativos, de prueba y de desarrollo	→	8.31	Separación de los entornos de desarrollo, prueba y producción.
12.2.1	Controles contra el malware	→	8.7	Protección contra malware
12.3.1	Respaldo de información	→	8.13	Copia de seguridad de la información

12.4.1	El registro de eventos	→	8.15	Inicio sesión
12.4.2	Protección de la información de registro	→	8.15	Inicio sesión
12.4.3	Registros de administrador y operador	→	8.15	Inicio sesión
12.4.4	Sincronización del reloj	→	8.17	Sincronización del reloj
12.5.1	Instalación de Software en Sistemas Operativos	→	8.19	Instalación de software en sistemas operativos.
12.6.1	Gestión de Vulnerabilidades Técnicas	→	8.8	Gestión de vulnerabilidades técnicas.
12.6.2	Restricciones en la instalación de software	→	8.19	Instalación de software en sistemas operativos.
12.7.1	Controles de auditoría de sistemas de información	→	8.34	Protección de los sistemas de información durante las pruebas de auditoría.
13.1.1	Controles de red	→	8.20	Seguridad de redes
13.1.2	Seguridad de los servicios de red	→	8.21	Seguridad de los servicios de red.
13.1.3	Segregación de Redes	→	8.22	Segregación de redes
13.2.1	Políticas y procedimientos de transferencia de información	→	5.14	Transferencia de información
13.2.2	Acuerdos sobre Transferencia de Información	→	5.14	Transferencia de información
13.2.3	Mensajería Electrónica	→	5.14	Transferencia de información
13.2.4	Acuerdos de confidencialidad o no divulgación	→	6.6	Acuerdos de confidencialidad o no divulgación
14.1.1	Análisis y especificación de requisitos de seguridad de la información.	→	5.8	Seguridad de la información en la gestión de proyectos.
14.1.2	Protección de servicios de aplicaciones en redes públicas	→	8.26	Requisitos de seguridad de la aplicación
14.1.3	Protección de transacciones de servicios de aplicaciones	→	8.26	Requisitos de seguridad de la aplicación
14.2.1	Política de desarrollo seguro	→	8.25	Ciclo de vida de desarrollo seguro
14.2.2	Procedimientos de control de cambios del sistema	→	8.32	Gestión del cambio
14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma operativa	→	8.32	Gestión del cambio
14.2.4	Restricciones sobre cambios en paquetes de software	→	8.32	Gestión del cambio
14.2.5	Principios de ingeniería de sistemas seguros	→	8.27	Principios de ingeniería y arquitectura de sistemas seguros
14.2.6	Entorno de desarrollo seguro	→	8.31	Separación de los entornos de desarrollo, prueba y producción.
14.2.7	Desarrollo subcontratado	→	8.30	Desarrollo subcontratado
14.2.8	Pruebas de seguridad del sistema	→	8.29	Pruebas de seguridad en desarrollo y aceptación.
14.2.9	Pruebas de aceptación del sistema	→	8.29	Pruebas de seguridad en desarrollo y aceptación.
14.3.1	Protección de datos de prueba	→	8.33	Información de prueba

15.1.1	Política de Seguridad de la Información para las Relaciones con Proveedores	→	5.19	Seguridad de la información en las relaciones con proveedores
15.1.2	Abordar la seguridad en los acuerdos con proveedores	→	5.20	Abordar la seguridad de la información en los acuerdos con proveedores
15.1.3	Cadena de suministro de tecnologías de la información y las comunicaciones	→	5.21	Gestión de la seguridad de la información en la cadena de suministro de TIC
15.2.1	Seguimiento y Revisión de Servicios de Proveedores	→	5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores.
15.2.2	Gestión de cambios en los servicios del proveedor	→	5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores.
16.1.1	Responsabilidades y Procedimientos	→	5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información.
16.1.2	Notificación de eventos de seguridad de la información	→	6.8	Informes de eventos de seguridad de la información
16.1.3	Informar las debilidades de la seguridad de la información	→	6.8	Informes de eventos de seguridad de la información
16.1.4	Evaluación y Decisión sobre Eventos de Seguridad de la Información	→	5.25	Evaluación y decisión sobre eventos de seguridad de la información.
16.1.5	Respuesta a Incidentes de Seguridad de la Información	→	5.26	Respuesta a incidentes de seguridad de la información
16.1.6	Aprender de los incidentes de seguridad de la información	→	5.27	Aprender de los incidentes de seguridad de la información
16.1.7	Recopilación de pruebas	→	5.28	Recopilación de pruebas
17.1.1	Planificación de la continuidad de la seguridad de la información	→	5.29	Seguridad de la información durante la interrupción
17.1.2	Implementación de la continuidad de la seguridad de la información	→	5.29	Seguridad de la información durante la interrupción
17.1.3	Verificar, revisar y evaluar la continuidad de la seguridad de la información	→	5.29	Seguridad de la información durante la interrupción
17.2.1	Disponibilidad de instalaciones de procesamiento de información	→	8.14	Redundancia de instalaciones de procesamiento de información.
18.1.1	Identificación de la legislación aplicable y requisitos contractuales	→	5.31	Requisitos legales, estatutarios, reglamentarios y contractuales
18.1.2	Derechos de propiedad intelectual	→	5.32	Derechos de propiedad intelectual
18.1.3	Protección de registros	→	5.33	Protección de registros
18.1.4	Privacidad y protección de la información de identificación personal	→	5.34	Privacidad y protección de la PII
18.1.5	Regulación de controles criptográficos	→	5.31	Requisitos legales, estatutarios, reglamentarios y contractuales
18.2.1	Revisión independiente de la seguridad de la información	→	5.35	Revisión independiente de la seguridad de la información.
18.2.2	Cumplimiento de Políticas y Estándares de Seguridad	→	5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información

			5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información
18.2.3	Revisión de cumplimiento técnico	→	8.8	Gestión de vulnerabilidades técnicas.