VINCI COMPASS

Políticas de Seguridad de la Información y Ciberseguridad V.3

Diciembre 2024

CONTENIDO

Control de cambios

Versión	Observación	Fecha	Creado / modificado
V.1	Creación del documento, inclusión de políticas como marco normativo, normas, principios, roles & responsabilidades y gobierno de seguridad de la información.	13-08-2018	Angelica Trujillo
V.2	Se incluyen lineamientos de ciberseguridad en el alcance, responsabilidad, marco de referencia, activos de información, concientización y capacitación, y el reporte de incidentes.	04-11-2021	Gabriel Bendezú
V.3	Se incorpora el rol y funciones de ciberseguridad, también el procedimiento de implementación y mantenimiento del SGSI.	06-11-2024	Gabriel Bendezú Pablo Cornejo

Historial de aprobación

Versión	Aprobador	Fecha aprobación	Ítem aprobado
V.1	Directorio	Diciembre 2018	Contenido del documento
V.2	Directorio	Diciembre 2021	Contenido del documento
V.3	Maria Isabel Bahamón	Noviembre 2024	Formato
V.3	Directorio	Noviembre 2024	Contenido del documento

(*) La presente versión sustituye completamente a todas las precedentes, de manera que éste sea el único documento válido de entre todos los de la serie.

1. GENERALIDADES

• Objetivo

La Política de Seguridad de la Información y Ciberseguridad provee un marco normativo para Vinci Compass y sus filiales, donde se detalla los principios, objetivos, y las acciones requeridas para proteger y administrar la seguridad de la información en base a la confidencialidad, integridad y disponibilidad. La definición de las bases para construir un marco de gestión de seguridad de la información estará acorde a la estructura interna de Vinci Compass y adhiriéndose a las buenas prácticas en la materia tales como el estándar ISO/IEC 27001 y los CIS Controls.

• Alcance

Las políticas aplican a todos los colaboradores de Vinci Compass, grupos contingentes y subcontratistas, indiferente al tipo vinculación laboral ya sea indefinida, plazo fijo u honorarios, quienes tienen acceso a la información y a los sistemas de información, de Vinci Compass.
El alcance de ciberseguridad comprenderá a todos los activos de información de Vinci Compass que se encuentren expuestos a internet dando prioridad a los activos más críticos para el negocio.

• Sanciones

Vinci Compass se reserva el derecho de iniciar acciones legales o disciplinarias según corresponda, hacia personas naturales o jurídicas cuyo accionar no se adhiera a la presente política.

• Adhesión a las Políticas

La seguridad de información y ciberseguridad requiere de la participación y el apoyo de todos, tanto internos como externos. En este sentido, todos los colaboradores deben usar y proteger apropiadamente los activos de información, cumpliendo lo dispuesto en el marco normativo compuesto por normas, procedimientos u otros documentos de Seguridad de la Información y Ciberseguridad que se generen a partir de estas políticas y que cumplan para este fin.

• Excepciones

Las excepciones a cualquier cumplimiento a las políticas de Seguridad de la Información y Ciberseguridad deben ser analizadas por el Oficial de Seguridad de la Información, además serán informadas al Comité de Seguridad de la Información. Todas las excepciones a las políticas deben ser formalmente documentadas, registradas y revisadas.

• Referencias Normativas

Para el presente documento y todos aquellos que forman parte del marco normativo se consideró como referencia el estándar ISO/IEC 27001 e ISO/IEC 27002. Para el cumplimiento de las disposiciones referentes a ciberseguridad se tomará como referencia los CIS Controls (Center for Internet Security Controls).

• Glosario de términos

○ **Activo de Información**	Algoritmo de cifrado simétrico avanzado de 256 bits que garantiza un alto nivel de seguridad para proteger datos sensibles.
○ **Ciberespacio**	Entorno virtual en el cual se transmiten información mediante la conexión a la red de internet y ordenadores.
○ **Información**	Cualquier forma de registro electrónico, óptico, magnético o en otros medios similares, susceptible de ser procesada, distribuida y almacenada.
○ **Confidencialidad**	Característica por la que la información no está disponible o no ha sido divulgada a individuos, entidades, o a procesos desautorizados. El acceso a la información confidencial es por parte únicamente de quienes estén autorizados.
○ **Integrida**d	Característica de salvaguardar la exactitud y completitud de los activos.
○ **Disponibilidad**	Característica de ser accesible y usable sobre demanda por una entidad autorizada.
○ **Seguridad de la Información**	Conjunto de medidas preventivas y reactivas que deben ser implementadas en la compañía, que permiten resguardar y proteger la información para mantener su confidencialidad, disponibilidad e integridad.

○ **Ciberseguridad**	Conjunto de medidas preventivas y reactivas que garantizan la protección de la información digital en los que reside los sistemas de información de la compañía y salvaguarda nuestros activos ante cualquier ataque cibernético.
○ **Usuario**	Es toda persona natural o jurídica a la cual se le concede autorización para acceder a lugares físicos, a la información y a los sistemas de Vinci Compass, incluye a todos los colaboradores o terceros que presten servicios y/o que realicen cualquier actividad en la Compañía.
○ **Propietario de Información**	Es quien define y determina la clasificación de seguridad y niveles de acceso a la información.
○ **Custodio de información**	Es quien gestiona los controles de seguridad de la información acorde a lo establecido por los propietarios de información.
○ **Incidente de Seguridad de la Información y Ciberseguridad**	Evento asociado a un incumplimiento de la política de seguridad y ciberseguridad, una falla en los controles, o una situación previamente desconocida relevante para la seguridad, que tiene una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la Información y ciberseguridad.
○ **Sistema de Gestión de Seguridad de la Información y Ciberseguridad SGSI-C**	Conjunto de elementos interrelacionados (estructura organizativa, políticas, planificación, responsabilidades, procedimientos, recursos, procesos) que utiliza una organización para establecer políticas, objetivos de seguridad de la información y ciberseguridad, y alcanzar dichos objetivos, basados en un enfoque de gestión y de mejora continua.

2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (POL1)

La política de Seguridad de la Información y Ciberseguridad apunta a asegurar la confidencialidad, integridad y disponibilidad de los activos de información. De esta política se emergen normas fundamentales, procedimientos y otros que cubren ámbitos de recursos humanos, seguridad lógica, adquisición, desarrollo y mantenimiento de sistemas, seguridad física y otros en referencia a los dominios indicados en el estándar ISO/IEC27001:2013 y CIS Controls para la implementación de SGSI-C. Las normas fundamentales que emanan de las políticas de Seguridad de la Información y Ciberseguridad se encuentran detalladas en el Anexo I. “Lista de Normas”.

2.1 De los Principios Generales

Para Vinci Compass la seguridad de la información y ciberseguridad:

1. Añade valor:

La seguridad y ciberseguridad agrega valor a los servicios y productos. La protección de los activos de información además de restricciones de acceso contempla medidas de seguridad que permitan mantener la información crítica integra y disponible para el normal desarrollo de las operaciones del negocio, conservando un adecuado balance costo beneficio entre las medidas de seguridad implementadas y los costos de no contar con la información exacta e integra en el momento requerido.

2. Es transversal:

La seguridad en Vinci Compass aplica a todas las áreas. Además, todos los Country head, Gerentes, Subgerentes y jefes, en sus áreas de responsabilidad, deberán alinear los niveles de protección de su información estratégica de acuerdo con las disposiciones de seguridad de la información y ciberseguridad que emanen del Comité de Seguridad de la Información.

3. Es parte de la cultura corporativa:

Se requiere crear y mantener los conceptos, conductas y acciones en relación con seguridad de la información y ciberseguridad.

4. Se construye por todos con un esfuerzo permanente:

La seguridad se logra porque todos los colaboradores, en todas las actividades que realicen, se incluye las condiciones de seguridad necesarias.

5. Requiere de una responsable asignación de recursos:

Dada la importancia que tiene para Vinci Compass la seguridad, se dedicaran recursos humanos y financieros que sean requeridos, con el objetivo de mantener e incrementar el nivel de seguridad de la información y ciberseguridad de forma corporativa.

6. Esta acorde a las exigencias del medio:

La implementación de seguridad debe estar conforme a las leyes aplicables, regulaciones, exigencias y estándares de la industria como, mínimo. Se establecerán objetivos y procedimientos propios cuando sea apropiado.

2.2 De la Protección de Activos

Seguridad de la Información y Ciberseguridad es la protección de los activos de la información por medio de controles a nivel organizacional y técnicos incluyendo políticas, normas y procedimientos, estructura organizacional, software, hardware y controles físicos. Como decisión estratégica Vinci Compass ha decidido establecer, implementar, mantener y mejorar de manera continua el SGSI-C en base al estándar ISO/IEC 27001 y los CIS Controls.

1. La seguridad de la información y ciberseguridad se debe entender como la preservación de su:
   - Confidencialidad: Asegurar que la información sea accesible solo al personal autorizado.
   - Integridad: Proteger la exactitud y completitud de la información.
   - Disponibilidad: Asegurar que los usuarios autorizados tengan acceso a la información y activos asociados cuando sea requerido.
2. La información y los sistemas de información de Vinci Compass son activos que tienen valor y, por lo tanto, como cualquier otro activo, requieren de una protección adecuada en todo momento. La Dirección de Vinci Compass considera necesario proteger apropiadamente a los activos de información de los riesgos que los pueden afectar de manera que se mantenga la confidencialidad, integridad y disponibilidad de la información, dentro de una evaluación permanente de las amenazas a las que se encuentra expuesta.
3. La implementación de la seguridad de la información y ciberseguridad se basa en un enfoque de administración de riesgos, permitiendo la identificación, cuantificación y priorización de los riesgos en base a los criterios establecidos en la aceptación de los mismos. Con este fin se utilizará como guía lo definido en el estándar ISO/IEC 27001 y los CIS Controls.
4. Sobre la selección de controles de seguridad que deben ser implementados, se tomará como base lo establecido en la norma ISO 27002 y los CIS Controls.

5. En Vinci Compass, las personas son un principal activo el cual también debe ser protegido. Todos los Country Head, Gerentes, Subgerentes y jefes de área, en conjunto con la Gerencia de Gestión y Desarrollo del Talento, y el Comité de Seguridad de la Información, deben realizar los esfuerzos necesarios con la finalidad de asegurar que todos los colaboradores reciban una adecuada capacitación para concientizar la importancia de la seguridad de la información y ciberseguridad en Vinci Compass.
6. Los activos de información deberán contar con propietarios de la información, responsables de la seguridad de los mismos.
7. Vinci Compass considera necesario resguardar, en especial, la divulgación de información confidencial relacionada con sus clientes y, por lo tanto, ésta debe ser protegida evaluando su sensibilidad, valor y criticidad. Esta protección incluye una restricción de acceso a la información, que se basa en el principio de que los colaboradores sólo deben tener acceso a aquella información que requieran para el ejercicio de sus funciones y habiendo sido previamente autorizados.
8. El periodo por el cual se mantendrá almacenada la información estará en función de las necesidades operativas y de los órganos de control, y de lo establecido según los requisitos legales, regulatorios y las obligaciones contractuales vigentes.

- Vinci Compass establece que se deben realizar los esfuerzos necesarios que permitan que la información esté disponible aún en situaciones de contingencia, para posibilitar la continuidad operativa de los negocios, además de proteger los activos y procesos críticos, de los efectos de fallas en los sistemas de información o desastres

2.3 De Roles y Responsabilidades Generales

a) El Comité de Seguridad de la Información (CSI) revisa, evalúa y propone a la Dirección las políticas, metodologías y responsabilidades generales en materia seguridad de información y ciberseguridad elaboradas por el Oficial de Seguridad de la Información (OSI), para su revisión y posterior aprobación del Directorio.
b) El Oficial de Seguridad de la información es responsable de elaborar, promover y coordinar las acciones e iniciativas de seguridad y ciberseguridad, continuidad de negocio y riesgo a nivel corporativo de Vinci Compass. Además de crear y actualizar periódicamente el marco normativo.
c) Los Country head de cada país, Gerentes, Subgerentes y jefes de área son los principales responsables de que al interior de sus áreas de trabajo y respectivos ámbitos se respeten las políticas, normas, estándares de seguridad y ciberseguridad, y los procedimientos asociados.
d) El especialista de Ciberseguridad es responsable de la ejecución, monitoreo y control de las iniciativas en materia de seguridad y ciberseguridad, las que incluyen, pero no se limitan a

gestión y mitigación de vulnerabilidades, respuesta a alertas e incidentes, evaluación de riesgos, protección de activos e información, supervisión de proveedores, entre otros.

e) Es responsabilidad de todos los colaboradores de Vinci Compass trabajar respetando las políticas, normas y procedimientos de seguridad y ciberseguridad definidos, en especial realizando los controles definidos para mitigar los riesgos.
f) Todo colaborador accederá a la información que sea estricta y exclusivamente necesaria para cumplir sus funciones.
g) Todo colaborador tiene la obligación de notificar sobre cualquier actividad o situación que afecte a la seguridad y ciberseguridad de los activos de información de Vinci Compass.

3. POLÍTICA DE GOBIERNO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (POL2)

La presente política tiene como objetivo el definir los roles y responsabilidades de los equipos y colaboradores en el contexto de la seguridad de la información y ciberseguridad.

3.1 Compromiso del Directorio y Comité sobre Seguridad de la Información

a) Vinci Compass conformará un equipo de trabajo ejecutivo para gestionar, evaluar y resolver sobre materias relacionadas a la Seguridad de la Información y Ciberseguridad, el que se denominará Comité de Seguridad de la Información (CSI).
b) Se crea el rol de Oficial de Seguridad de la Información (OSI), quien debe promover, evaluar y fiscalizar las medidas de seguridad aprobadas por el CSI. El rol del OSI podrá ser asumido por una persona jerárquicamente independiente de las unidades organizacionales existentes y con el debido nivel organizacional para poder gestionar la Seguridad de la Información y Ciberseguridad en Vinci Compass, o bien, podrá ser asignado a alguna persona que no comprometa ética ni funcionalmente el ejercicio de las funciones que desempeña.
c) Los responsables de las distintas áreas deberán cerciorarse de que la seguridad de la información y ciberseguridad es tratada como parte del negocio y que los desafíos asociados a ella son encarados y resueltos, tal y como se hace para los demás problemas del negocio.
d) Es deber de todas las jefaturas evaluar periódicamente su entorno laboral, con el objetivo de identificar riesgos asociados a la Seguridad de la Información y Ciberseguridad.
e) El Directorio deberá definir el nivel de riesgo aceptable para los riesgos que se identifiquen y deberá determinar las acciones a tomar para gestionarlo, a través de alguna de las siguientes alternativas:

    - Evitar: Eliminar completamente la exposición a determinados riesgos.
    - Mitigar: Aumentar los controles sobre el riesgo para incrementar la mitigación ya sea reduciendo la probabilidad de ocurrencia o su nivel de impacto.
    - Transferir: Tercerizar el riesgo, delegar la responsabilidad de gestión a otros en pro de continuar con la mitigación de otros riesgos potenciales al interior de la Compañía.
    - Aceptar: Pueden ser aceptados en los casos en que se encuentren dentro del nivel de TOLERANCIA y el costo de mitigarlos sea mayor que la propia pérdida estimada.

3.1.1. Coordinación de la Seguridad de la Información y Ciberseguridad en Filiales

Las actividades de la Seguridad de la Información y Ciberseguridad en cada filial deberán realizarse de manera coordinada por el OSI, Directorios, Country Head de cada país, equipos de trabajos definidos para Seguridad de la Información y Ciberseguridad locales, además de gerencias, jefaturas locales y de las diferentes áreas involucradas.

3.1.2. Evaluación de los Riesgos de Seguridad de la Información y Ciberseguridad

Vinci Compass deberá aplicar procedimientos para la evaluación de los riesgos de seguridad de la información y ciberseguridad que se podrían estar asumiendo al introducir nuevos productos, sistemas, emprender nuevas actividades o definir nuevos procesos.

3.2. Roles y Responsabilidades Específicos

Vinci Compass mantendrá un registro de los perfiles y cantidad necesaria de personas con conocimientos comprobables en estándares de Seguridad de la Información y Ciberseguridad.

3.2.1. Directorio

Las responsabilidades de la junta directiva en relación con la gestión de la seguridad de la información y ciberseguridad serán:

a) Aprobar las políticas de Seguridad de la Información y Ciberseguridad.
b) Apoyar las políticas, normas, planes y/o programas u otras iniciativas para impulsar la gestión de Seguridad de la Información y Ciberseguridad promoviendo la cultura en Vinci Compass.
c) Conocer los principales riesgos de seguridad y ciberseguridad afrontados por Vinci Compass y definir el riesgo aceptable.

3.2.2. Comité de Seguridad de la Información (CSI)

Las responsabilidades del Comité de Seguridad de la Información (CSI) en relación con la Gestión de la Seguridad de la Información y Ciberseguridad serán:

a) Reportar al Directorio sobre nuevas políticas o cambios que se presenten en el marco normativo. Además de reportar los riesgos para su aprobación.

b) Analizar la gestión de riesgos, y ver posibles acciones presentadas por el Oficial de Seguridad.
c) Supervisar la ejecución de políticas, aprobar normas, planes de seguridad, metodologías y/o marcos de referencia asociados a seguridad de la información y ciberseguridad, analizar cambios significativos del nivel de exposición al riesgo y apoyar en la toma de decisiones cuando se le solicite.
d) Guiar las funciones del Oficial de Seguridad de la Información y aprobar o nombrar interlocutores específicos para el desarrollo de proyectos de Seguridad de la Información y Ciberseguridad.
e) Promover la difusión, apoyo y concientización de la seguridad de la información y Ciberseguridad.
f) Normar la ejecución de auditorías internas y externas referentes a la Seguridad de la Información y Ciberseguridad de Vinci Compass.

3.2.3. Requerimientos de Constitución del CSI

a) El quorum del Comité es la mitad más uno de sus miembros. En caso el número sea impar, el quorum es el número entero inmediato superior al de la mitad de aquel.
b) Los acuerdos adoptados y temas tratados quedarán documentados en un acta, además de una presentación que incluye los temas a tratar.
c) Los miembros del comité se encuentran definidos en el Reglamento del Comité.

3.2.4. Oficial de Seguridad de la Información (OSI)

El Oficial de Seguridad de la Información (OSI) trabajará estrechamente con el Comité de Seguridad de la Información CSI planteando estrategias de implementación de planes y/o programas con relación a la materia. Dentro de sus funciones principales se incluye:

a) Definir y/o proponer las políticas, procedimientos, metodologías, herramientas, procesos y responsabilidades referidas a la Seguridad de Información y Ciberseguridad al CSI.
b) Monitorear y reportar a CSI el nivel de cumplimiento de las actividades y funciones de Seguridad de la Información y Ciberseguridad.
c) Mantener custodia, además de difundir y mantener la actualización de las políticas de seguridad de la información y ciberseguridad.
d) Identificar requerimientos de Seguridad de la Información y Ciberseguridad, y propondrá e informará al CSI sobre temas e iniciativas a desarrollar dentro del ámbito de Seguridad de la Información y Ciberseguridad.
e) Deberá evaluar, coordinar y monitorear la implementación de controles de seguridad de la información para los activos de información existentes y nuevos.

f) Identificar y evaluar amenazas y vulnerabilidades de la Seguridad de la Información y Ciberseguridad a fin de identificar los controles a implementar.
g) Supervisar la creación y actualización, además de la custodia, del inventario de activos de información en coordinación con los propietarios de la información de Vinci Compass.
h) Definir la estrategia de capacitación y entrenamiento con relación a la Seguridad de la Información y Ciberseguridad. Así como preparar y coordina dichos programas de capacitación.
i) Elaboración y actualización del Plan de Tratamiento de Riesgos.
j) Elaborar, con el apoyo de los dueños de procesos y en base a las políticas, indicadores de gestión de la Seguridad de la Información y Ciberseguridad para cada una de las áreas relevantes. Monitorear e informar periódicamente al Comité de Seguridad de la Información el desempeño de éstos.
k) Participar y contribuir en la aplicación de la metodología para el mantenimiento de los planes de contingencia y continuidad del negocio.
l) Mantener un conocimiento actualizado de las metodologías, estándares, herramientas y soluciones relacionadas a la Seguridad de la Información y Ciberseguridad. Aplicar estos conocimientos en forma eficiente y efectiva.
m) Coordinar las sesiones o reuniones del Comité de Seguridad de la Información, ya sean de carácter ordinario o extraordinario.

3.2.5. Ciberseguridad

El especialista de ciberseguridad trabajara junto con el Oficial de Seguridad de la Información y el equipo de Soporte e Infraestructura para mantener la seguridad y ciberseguridad en niveles óptimos. Dentro de sus principales funciones se incluyen:

a) Administrar las plataformas de seguridad y ciberseguridad
b) Gestión y mitigación de vulnerabilidades
c) Elaboración y seguimiento de indicadores de riesgo KRI.
d) Revisión y actualización de políticas, normas y procedimientos.
e) Seguimiento y respuesta a incidentes.
f) Supervisión de servicios de ciberseguridad tercerizados.
g) Análisis forense de incidentes.
h) Evaluación de riesgos y controles de ti.
i) Atender requerimientos de auditoria normativos y regulatorios.
j) Ejecución y control de pruebas de seguridad y ciberseguridad.

3.2.6. Propietario de la información

El Propietario de la Información, en relación con la Gestión de la Seguridad de la Información y Ciberseguridad es quien define y determina la clasificación de seguridad y los niveles de acceso a la información. Para el cumplimiento de esta responsabilidad se han dispuesto las siguientes actividades:

a) Sugerir y apoyar en la elaboración de las políticas, normas y procedimientos de Seguridad de la Información y Ciberseguridad dentro de sus respectivas áreas y procesos.
b) Definir la clasificación de la información de Vinci Compass dentro de sus respectivas áreas y procesos.
c) Revisar periódicamente la clasificación de la información dentro de sus respectivas áreas y procesos y reclasificar y desclasificar en los casos que la información lo amerite.
d) Mantener actualizado el inventario de activos de información dentro sus respectivas áreas y procesos. Esto incluye a los activos del ciberespacio.
e) Supervisar periódicamente los niveles de acceso a los sistemas de información.
f) Informar al OSI cualquier posible incidente de seguridad y ciberseguridad que se detecte en la información bajo su responsabilidad y velar que se realicen las investigaciones necesarias.
g) Supervisar que se apliquen los controles de seguridad solicitados.
h) Definir los roles y perfiles de usuarios de acuerdo con las necesidades de su proceso y/o área, en coordinación con el OSI.
i) Autorizar los permisos de acceso a la información y a los sistemas de información y relevantes a sus funciones.

3.2.7. Custodia de la Información

La principal responsabilidad del Custodio de la Información en relación con la Gestión de la Seguridad de la Información y Ciberseguridad es proteger la información de la distribución, acceso, modificación, destrucción y/o uso no autorizado en base a lo indicado por el Propietario de la información.
Para el cumplimiento de esta responsabilidad se han dispuesto las siguientes actividades:

a) Administrar los controles relevantes a la Seguridad de la Información y Ciberseguridad, acorde a las instrucciones establecidas por los Propietarios de la Información (mecanismos de resguardo, validación de autenticidad, restricción de acceso, otros)
b) Implementar controles físicos o técnicos.
c) Administrar el acceso a la información.

d) Cumplir con los controles implementados para la protección de la información asignada para su custodia.
e) Asegurar la disponibilidad de la información a través de mecanismos de recuperación adecuados y acordes a la criticidad de la información bajo su responsabilidad e indicados por los Propietarios de la Información.

3.2.8. Usuario de la Información

La principal responsabilidad de los usuarios de la información en relación con la Gestión de la Seguridad de la Información y Ciberseguridad es cumplir con las políticas de seguridad de la información y ciberseguridad.
Son los colaboradores o personal externo de apoyo, quienes utilizan la información en sus actividades habituales. Las funciones referentes a la seguridad de información y ciberseguridad son:

a) Cumplimiento a las políticas y procedimientos de seguridad de la información y ciberseguridad.
b) Mantener la confidencialidad de su cuenta y contraseñas para el acceso a aplicaciones, sistemas de información y recursos informáticos.
c) Utilizar la información de Vinci Compass sólo para el cumplimiento de sus funciones y/o para fines organizacionales.
d) Reportar eventos y/o incidentes a través de los canales de reporte.
e) En caso de identificar brechas u oportunidades de mejora, debe comunicarlas al OSI.
f) Solicitar respaldo de la información crítica que utiliza fuera de los sistemas de información al Área de Soporte.

De manera complementaria, se establecerán funciones y estructuras en las Normas de Seguridad de la Información y Ciberseguridad.

3.3. Acuerdos y/o Cláusulas Contractuales

Vinci Compass, a través de sus asesores legales, identificará y revisará que los requerimientos de seguridad de la información y ciberseguridad sobre necesidad de establecer la confidencialidad, con el fin de proteger la información tanto para los colaboradores y relaciones con partes externas. Para tal fin, se establecerán acuerdos contractuales que definan las responsabilidades en materia de seguridad de la información y ciberseguridad, incluyendo sanciones. Estos acuerdos deben incluir la revocación de derechos de acceso y devolución de activos ante un cambio de posición o desvinculación del colaborador.

Para proveedores, las condiciones considerarán al menos los siguientes elementos: protección de la información, duración del acuerdo, acciones requeridas al terminar el servicio, responsabilidades de los firmantes para evitar la divulgación de la información, propiedad de la información, uso permitido de la información confidencial, condiciones para el retorno o destrucción de la información y acciones esperadas a realizar en caso de incumplimiento del acuerdo.

Los acuerdos y/o cláusulas de confidencialidad deberán cumplir con todas las leyes y regulaciones aplicables. Los acuerdos serán aplicables a toda relación ya sea contractual o por servicios específicos con partes externas tales como proveedores, asesores, u otros.

3.4. Contacto con las Auditorias

Vinci Compass deberá contar con un proceso que especifique cuándo, cómo y cuáles autoridades contactar. Todos aquellos contactos con autoridades deben ser previamente comunicados a los asesores legales y al Gerente respectivo.
Vinci Compass a través de la Gerencia involucrada, Gerencia Tecnología, Gerencia de Legal & Compliance, y/o el Oficial de Seguridad deberán mantener una relación con las entidades externas que puedan prestar apoyo en caso de incidentes de seguridad y ciberseguridad. La relación deberá mantenerse a un nivel tal que asegure el apoyo, pero sin generar obligaciones de entregar información.

3.5. Manejo de Seguridad en Relación con Partes Externas

Vinci Compass deberá contar con los mecanismos y procedimientos necesarios para identificar los riesgos para la información que involucren a las partes externas, ya sean proveedores, asesores u otros, considerando documentos legales, como los contratos, y se debe tomar las medidas necesarias tales como acuerdos de confidencialidad mencionado en la sección 3.3, y/o la implementación de controles adecuados antes de permitir el acceso.

3.6. Manejo de la Seguridad en la Relación con los Clientes

Se protegerá la información de los clientes y a su vez los clientes resguardarán la información entregada por parte de Vinci Compass. Toda relación con clientes será por medio de un contrato de servicio, asesoría u otro acuerdo legal en donde se establece las obligaciones y responsabilidades de las partes.

4. APETITO DE RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

El apetito de riesgo en este aspecto se definirá en base a dos variables el porcentaje de indisponibilidad de sistemas críticos y el tiempo de remediación de vulnerabilidades según su criticidad. Para mayor detalle revisar la Política Integral de Gestión de Riesgo.

5. DISPOSICIONES FINALES

5.1 Implementación y Mantenimiento

Las políticas de seguridad de la información y ciberseguridad, de acuerdo con la fecha de aprobación, tendrán un periodo de implementación no mayor a un año. Las políticas serán revisadas por el Comité de Seguridad de la Información (CSI) de Vinci Compass y aprobadas por el Directorio.
El nivel de cumplimiento estará condicionado a que las normas, procedimientos u otros documentos que soportan su cumplimiento, queden operativos, los mismos que deberán contar con un adecuado registro para la correcta gestión de la seguridad de la información, así como mantener una suficiente evidencia de auditoría.
El procedimiento de implementación y mantenimiento consiste en hacer una revisión anual de las políticas, normas y procedimientos que comprenden todo el sistema de gestión. Esto permite confirmar que el objetivo y alcance sean relevantes, actuales y alineados con los requerimientos técnicos, legales, gubernamentales y del negocio. Además, que se encuentren alineados con el estándar ISO 27001 y también con los CIS CONTROLS de seguridad de la información y Ciberseguridad respectivamente.
Los cambios mayores y/o creación de políticas requieren aprobación del directorio, y en el caso de normas y procedimientos a nivel de comité. En el caso de cambios menores estos pueden ser realizados como parte de una revisión anual y no requieren una instancia de revisión y/o aprobación.

5.2 Distribución

Las políticas serán comunicadas internamente a todos los colaboradores y/o subcontratistas de Vinci Compass.

ANEXO I. LISTA DE NORMAS

Referencia	Norma	Objetivos
NOR01	Seguridad Recursos Humanos	Establecer mecanismos específicos para el control adecuado de candidatos potenciales para el empleo, para reducir el riesgo de error humano, el mal uso de recursos, robo y fraude. Reducir los daños ocasionados por incidentes de seguridad y ciberseguridad, y mal funcionamiento. Asegurar que los empleados estén conscientes de las amenazas de la seguridad de la información y que se comprometan con la política de seguridad de la organización, durante su trabajo normal.
NOR02	Seguridad Física y Ambiental	Definir áreas de seguridad con el objeto de impedir el acceso no autorizado, daños o interferencias a los activos de información dentro de Vinci Compass. Definir la seguridad física y ambiental en los equipos con el objeto de prevenir pérdidas, daños o compromiso de los bienes e interrupción de las actividades de Vinci Compass y evitar que sean robados o se comprometa la información o los equipos que la procesan o almacenan.
NOR03	Control de Acceso	Proporcionar seguridad razonable con respecto a la confidencialidad, integridad y disponibilidad de los sistemas y recursos de información, a través de un adecuado manejo y mantenimiento de las cuentas del usuario y los derechos y privilegios asociados con ellas, para acceder a los servidores, aplicaciones, bases de datos y datos.
NOR04	Gestión de la continuidad del Negocio	Proteger a las personas dentro de las dependencias de Vinci Compass tanto en situación normal como en situación derivada de un desastre. Mantener la integridad y la disponibilidad de los activos de información, minimizando su pérdida ante eventuales desastres que interrumpan algún proceso de negocio o servicios críticos, por lo que existirán las habilidades para recuperar y reanudar la operación en el nivel y plazo acordado. Cumplir con aspectos legales, normativos y contractuales. Mejorar de forma continua la continuidad operacional.
NOR05	Gestión de Activos de Información	Definir los criterios que deben existir para identificar y clasificar la información de Vinci Compass.
NOR06	Cumplimiento Legal y Contractual	Definir aspectos de cumplimiento de regulaciones internas y externas. Evitar infracciones a las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la Seguridad de la Información y de los requisitos de seguridad.
NOR07	Gestión de Infraestructura TI y Comunicaciones	**No vigente**, fue reemplazada por la Política de Tecnología de Información y Comunicación (TIC).

Referencia	Norma	Objetivos
NOR08	Gestión de Incidentes	Asegurar que los eventos y debilidades de Seguridad de la Información asociados a los sistemas de información sean comunicados oportunamente, lo cual permita tomar acciones correctivas a tiempo. Asegurar una eficaz gestión de incidentes de seguridad de la información.
NOR09	Adquisición, Desarrollo y Mantención de Sistemas	Definir los lineamientos fundamentales para las actividades de sistemas ya sea su desarrollo, adquisición y/o mantención, garantizando que la seguridad de la información es parte integral de los sistemas de información.
NOR10	Contraseñas	Concientizar a los usuarios acerca de la importancia de la utilización, robustez y resguardo de las contraseñas como medida de seguridad, en todo proceso de comunicación realizado en los sistemas de información.
NOR11	Respaldos y Recuperación	Establecer lineamientos generales aplicables a los sistemas de información y a la infraestructura de servidores, en referencia a procedimientos de respaldos, recuperación y almacenamiento de la información para garantizar la disponibilidad e integridad de los activos de información de Vinci Compass.
NOR12	Gestión de parches y cambios	Establecer lineamientos generales aplicables a las actualizaciones de parches y alertas de seguridad, para minimizar los eventos maliciosos o posibles amenazas. Los parches críticos o recomendaciones de las alertas de seguridad deberán ser implementadas luego de validarse la compatibilidad de las aplicaciones existentes y en base a la toma de decisiones pertinentes según el caso.
NOR13	Sanitización y eliminación segura	Establecer lineamientos generales para la sanitización de medios de almacenamiento y eliminación segura de la información cuando no sea más requerida, siendo en formato de documentación impresa o medios de almacenamiento electrónico, de tal forma que los recursos de Vinci Compass y la información estén protegidas de amenazas de seguridad asociadas a la recuperación y reconstrucción de datos confidenciales.
NOR14	Ciberseguridad	Establecer lineamientos generales para la gestión de ciberseguridad en los sistemas de información que procesan, almacenan y transportan información digital de Vinci Compass expuesta a internet.
NOR15	Seguridad para proveedores	Establecer lineamientos generales para la protección de los activos de información accesibles a los proveedores y mantener un nivel acordado de seguridad de información y prestación de servicios conforme a los acuerdos con el proveedor.
NOR16	Privacidad	**No vigente**, fue reemplazada por la Política de Privacidad publicada en la web corporativa.
NOR17	Uso aceptable de recursos	Definir los lineamientos fundamentales para el uso aceptable de recursos de la Vinci Compass, incluye sin limitar, el uso de mail, internet, equipos de computación, laptops, sistemas de información, medios de almacenamiento, mensajería, entre otros. Garantizar la integridad, confiabilidad, disponibilidad y rendimiento de los recursos de la Vinci Compass.
NOR18	Tratamiento y gestión del riesgo	Definir el plan de tratamiento de riesgos que hacen parte del sistema de gestión de seguridad de la información, con el fin de aplicar los controles con los cuales se busca mitigar su materialización en Vinci Compass.