

DI-POL-SI0202

Seguridad de la Información

B&B Global

Documento Interno**Políticas Internas****Sistemas y Tecnología****Clasificación de la información: PUBLICA**

Historia de Revisión

Fecha	Nro. revisión	Descripción	Autor	Aprobó
02/07/2018	1	Creación de Política	Lionel Bo	Lionel Bo
01/06/2020	1.1	Referencia a DI-POL-200513A	Fernando González	Lionel Bo
07/06/2022	1.2	Clasificación	Fernando González	Andrés Racic
18/07/2024	1.3	Aprobación de la Dirección	Fernando González	Paul Buenader
24/07/2025	1.4	Revisión de la Política	Lionel Bo	Andrés Racic
01/09/2025	1.5	Actualización de formato y de documentos anexados	Thomas Capurro	Andrés Racic

Tabla de Contenidos

1. Objetivo	4
2. Consideraciones Generales	4
3. Alcance.....	4
4. Definiciones	4
4.1. Seguridad de la Información	4
4.2. Información	4
4.3. Sistema de Información.....	4
4.4. Tecnología de la Información.....	4
4.5. Gestión del Riesgo de la Seguridad de la Información.....	5
4.6. Incidente de Seguridad	5
5. Uso apropiado de los recursos.....	5
6. Gestión del Riesgo	5
7. Principales roles y responsabilidades	5
7.1. Dirección.....	5
7.2. Gerentes y jefes.....	5
7.3. Gerencia de Sistemas y Tecnología.....	6
7.4. Dueños de Información	6
7.5. Recursos Humanos	6
7.6. Legales	6
7.7. Usuarios	6
8. Seguridad de la información.....	7
8.1. Organización de la Gestión de Seguridad de la Información.....	7
8.2. Clasificación y Control de la información.....	7
8.3. Concientización del Personal	7
8.4. Seguridad Física y Ambiental.....	7
8.5. Gestión de comunicaciones y operaciones	7
8.6. Control de acceso a los sistemas de información.....	7
8.7. Desarrollo y mantenimiento de los sistemas	8
8.8. Gestión de incidentes de seguridad de la información.....	8

8.9. Asegurar el Cumplimiento.....	8
8.10. Capacitaciones al Personal	8
8.11. Requisito para Empleados, Consultores y Proveedores.....	8
9. Incumplimiento	8
10. Excepciones.....	8
11. Documentos complementarios	8

1. Objetivo

Establecer las pautas a seguir y las obligaciones a cumplir en materia de Seguridad de la Información, tendiente a proteger los activos de la compañía.

2. Consideraciones Generales

Una buena estrategia de Seguridad de la Información es contar con una Política implementada y documentada, donde se establezcan las pautas a seguir y las obligaciones a cumplir en materia de Seguridad de la Información y que además sirva como punto de partida para elaborar normas y procedimientos tendientes a proteger los activos de la compañía y la mejora continua del sistema de gestión de Seguridad de la Información.

3. Alcance

Todos los empleados de B&B Consultora S.A. y los terceros que interactúen con esta.

4. Definiciones

A los efectos de este documento se aplican las siguientes definiciones.

4.1. Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de Procesamiento
- **Disponibilidad:** se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

4.2. Información

Se refiere a un conjunto organizado de datos procesados, que se representan de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

4.3. Sistema de Información

Es un conjunto de elementos orientados al tratamiento y administración de datos e información que ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de la organización.

4.4. Tecnología de la Información

Hardware y software operados en el ámbito de la empresa o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Negocio.

4.5. Gestión del Riesgo de la Seguridad de la Información

Se entiende por gestión del riesgo de la seguridad de la Información (GRSI) al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

4.6. Incidente de Seguridad

Un incidente de seguridad es un evento adverso en un sistema o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

5. Uso apropiado de los recursos

El equipamiento informático, software e infraestructura de red que B&B Consultora S.A. pone a disposición de sus empleados, debe utilizarse para los propósitos de negocio para los que ha sido concebido. Además, la información que procesan estos recursos en propiedad de B&B Consultora S.A. y debe ser tratada de manera confidencial.

El uso apropiado de los recursos se encuentra detallado en el documento "**DI-POL-SI0206-Uso de Recursos**" complementario a esta política.

6. Gestión del Riesgo

Complementario a este documento, se cuenta con la política **DI-POL-SI0209-Gestión del Riesgo de Seguridad de la Información**", que indica los métodos utilizados para identificar los riesgos y evaluar la efectividad de sus mitigantes, minimizando el impacto en los procesos de la Empresa.

7. Principales roles y responsabilidades

7.1. Dirección

La dirección de B&B Consultora S.A. es responsable de definir los lineamientos y de comunicar la obligatoriedad de cumplimiento de las políticas de seguridad de la información, sus estándares y procesos asociados; y de delegar a la Gerencia de Sistemas y Tecnología la responsabilidad por el control y la verificación de que los procedimientos de seguridad sean realizados y cumplidos por todo el personal; Además es responsable de asignar los recursos para que se pueda llevar a cabo la implementación de las políticas definidas.

7.2. Gerentes y jefes

Los gerentes y jefes son responsables de la implementación y cumplimiento de la Política de Seguridad de la Información por parte de sus equipos de trabajo.

7.3. Gerencia de Sistemas y Tecnología

Tendrá entre sus principales funciones:

- ☐ Confeccionar la Política de Seguridad de la Información para ser presentada y aprobada por la Dirección de la Compañía.
- ☐ Difusión de la política.
- ☐ Presentar el Plan de Seguridad de la Información anual que contemple objetivos, actividades y presupuesto para llevar adelante la gestión de la seguridad de la información
- ☐ Llevar adelante una gestión eficiente de la seguridad de la Información basada en el cumplimiento de la presente Política
- ☐ Tomar iniciativas para incrementar la seguridad de la información en la Compañía
- ☐ Evaluar y coordinar la implementación de controles específicos de seguridad de la información para los sistemas o servicios.
- ☐ Promover la difusión de la presente Política.
- ☐ **El departamento de tecnología** cumplirá la función de cubrir los requerimientos de seguridad de la información establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Compañía.
- ☐ **El departamento de desarrollo** tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

7.4. Dueños de Información

Son los responsables de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de esta, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo con sus funciones y competencia.

7.5. Recursos Humanos

Cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, de los cambios que en ella se produzcan y la implementación de la suscripción al presente documento y sus anexos y al Compromiso de Confidencialidad.

7.6. Legales

Verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Compañía con sus empleados y con terceros. Asimismo, asesorará en materia legal, en lo que se refiere a la seguridad de la información.

7.7. Usuarios

Se requiere a los usuarios el conocimiento y cumplimiento de la presente política de seguridad de la información, normas, procedimientos y estándares aplicables. Deben entender completamente estos requisitos y actuar conforme a ellos.

8. Seguridad de la información

La información es un recurso que, como el resto de los activos, tiene valor para la Compañía y por consiguiente debe ser debidamente protegida.

Es importante que los principios de la Política de Seguridad de la Información sean parte de la cultura de la compañía. Para esto, se debe asegurar un compromiso manifiesto de la Dirección y de los Gerentes para la difusión, consolidación y cumplimiento de la presente Política.

Esta Política se conforma de una serie de pautas sobre aspectos específicos de la Seguridad de la Información, que incluyen los siguientes tópicos:

8.1. Organización de la Gestión de Seguridad de la Información

Orientado a definir roles y responsabilidades de acuerdo con las diferentes funciones que se desprendan de la gestión de la seguridad de la información. Establecer el marco de trabajo para la gestión del riesgo y delinear las condiciones y requisitos de seguridad para terceros que tengan accesos a información e instalaciones de procesamiento de esta.

8.2. Clasificación y Control de la información

Definir pautas generales para asegurar una adecuada clasificación, tratamiento y control de la información teniendo en cuenta los criterios de confidencialidad, integridad y disponibilidad de la información.

8.3. Concientización del Personal

Poner en conocimiento a empleados y terceros acerca del contenido de la presente política como así también los procesos disciplinarios que deriven de su cumplimiento, logrando crear conciencia del buen uso de los recursos informáticos de la compañía.

8.4. Seguridad Física y Ambiental

Realizar controles sobre la eficacia de las medidas de protección físicas implementadas para proteger instalaciones y equipos de procesamiento de información contra amenazas físicas, lógicas y/o ambientales que podrían afectar la seguridad de la información.

8.5. Gestión de comunicaciones y operaciones

Asegurar una correcta operación de las instalaciones de procesamiento de información, la integridad de las aplicaciones y la confidencialidad de las comunicaciones. Con el fin de alcanzar estos objetivos, se deben asignar responsabilidades y establecer controles técnicos y procedurales.

8.6. Control de acceso a los sistemas de información

Controlar el acceso a la información y a los sistemas que la procesan en base a los requisitos del negocio y de la seguridad; los mismos solo deben ser concedidos de acuerdo con la necesidad de conocimiento. Se debe prevenir a través de controles técnicos apropiados los accesos no autorizados a los sistemas de información.

8.7. Desarrollo y mantenimiento de los sistemas

Procurar un entorno de desarrollo seguro que cumpla con requisitos de seguridad en todas sus fases. Gestión de la continuidad del negocio
Desarrollar controles sobre los planes de recuperación ante desastres y de continuidad del negocio para garantizar el normal funcionamiento de las unidades de negocio y ambientes de tecnología ante una contingencia.

8.8. Gestión de incidentes de seguridad de la información

Una apropiada gestión de los incidentes de seguridad reduce al mínimo el daño causado por los mismos, permite el monitoreo y desarrollo de una base de conocimiento.

8.9. Asegurar el Cumplimiento

Instrumentar los mecanismos necesarios para la protección de la información de acuerdo con la legislación y regulaciones vigentes.

8.10. Capacitaciones al Personal

Toda modificación a esta política deberá incluir una capacitación al personal, asegurándose de que hayan comprendido los conceptos definidos en esta. Las mismas deben ser registradas y guardadas como evidencia del entendimiento.

8.11. Requisito para Empleados, Consultores y Proveedores

Antes de dar acceso o compartir información, todo Empleado, Consulto externo y/o Proveedor de B&B Consultora S.A. deberá firmar el documento **"DI-FOR-SI0208- Convenio de Confidencialidad"** el cual debe quedar archivado en su legajo.

9. Incumplimiento

En caso de incurrirse en el incumplimiento de esta política, o de las normas, procedimientos y estándares relacionados con la seguridad de la información; podrá ser pasible de sanciones disciplinarias. El área de Recursos Humanos analizará las medidas a implementar en caso de incumplimiento de la presente política.

10. Excepciones

Toda excepción a este documento deberá contar con la aprobación formal de la Dirección y quedar documentada de forma adecuada.

11. Documentos complementarios

Este documento hace referencia a los siguientes documentos que lo complementan:

DI-POL-SI0209-Gestión del Riesgo de Seguridad de la Información
DI-POL-SI0206-Uso de Recursos
DI-FOR-SI0208-Convenio de Confidencialidad