POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y USO DE ACTIVOS

BH COMPLIANCE

Destinatarios de esta política (la "Política")	Todos los usuarios de sistemas informáticos y de comunicaciones de BH Compliance, incluyendo trabajadores, contratistas y proveedores (en conjunto, los "Usuarios")
Objetivos	El propósito de la Política es definir los estándares para salvaguardar la información de BH Compliance y de sus Clientes contra el uso y divulgación no autorizados
Fecha de implementación	Abril 2021
Versión	1
Documentos Relacionados	Reglamento Interno de Orden, Higiene y Seguridad (trabajadores) Contrato de Trabajo (trabajadores) Contrato de Prestación de Servicios (proveedores)

1. ASPECTOS GENERALES

1.1. INTRODUCCIÓN

BH Compliance está consciente que la información es uno de sus activos más importantes, así como el de sus Clientes y que, al mismo tiempo, está expuesta a riesgos y amenazas que pueden provenir tanto desde dentro como fuera de la empresa.

1.2. OBJETIVOS

Esta Política tiene por objeto establecer los lineamientos generales para la definición, implementación, tratamiento y control de la seguridad lógica y física de los activos de información al interior de la empresa, para proteger su Confidencialidad, Integridad y permitir su Disponibilidad.

En particular, la Política busca:

- Proteger los activos de información de BH Compliance y, especialmente, la información de los Clientes, así como el correcto uso de ella, independientemente del soporte en el que se encuentre (papel o electrónico).
- Prevenir el acceso no autorizado a los sistemas de información de BH Compliance.
- Promover y concientizar a los destinarios de esta Política sobre la responsabilidad de BH Compliance, como organización, de proteger la información y su uso adecuado, así como todos los activos de BH Compliance.

1.3. ALCANCE

La Política es aplicable al uso de todos los activos de información, tangibles e intangibles de BH Compliance, que incluye no sólo la información de BH Compliance y de sus Clientes, sino que además todos los equipos, redes, tecnología y servicios a través de los cuales se accede o procesa tal información, que sean:

- Accedidos en o desde las instalaciones de BH Compliance;
- Accedidos de forma remota, desde cualquier fuente o plataforma;
- Accedidos mediante el uso de equipos de BH Compliance o controlados por BH Compliance.
- Usados de una forma que identifican a la persona que accede a los activos de información de BH Compliance.

La seguridad de la información es responsabilidad de todos. La observancia de esta Política por parte de los Usuarios de BH Compliance es esencial para la gobernanza, seguridad y gestión de los activos de información.

1.4. MARCO NORMATIVO

Las siguientes regulaciones -no taxativas- afectan el ámbito de seguridad de la información y a esta Política:

- Ley Nº 20.393 sobre responsabilidad penal de las personas jurídicas
- Ley Nº 19.223 sobre delitos informáticos

- Ley Nº 19.628 sobre protección de la vida privada
- Ley Nº 19.039 sobre propiedad industrial
- Ley Nº 17.336 sobre propiedad intelectual
- Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma

2. DEFINICIONES

2.1. Activo de Información: Cualquier información que tiene valor para BH Compliance y/o para sus Clientes, independiente del soporte en el que se encuentre, así como todos los dispositivos, equipos, software, tecnología, redes, servicios, medios, procedimientos y otros bienes, tangibles o intangibles, que procesan, almacenan, mantienen, protegen o controlan el acceso a la información dentro la organización.

2.2. Confidencialidad: La información solo debe ser divulgada a personas o procesos autorizados.

2.3. Clientes: Clientes de BH Compliance.

2.4. Disponibilidad: La información debe estar accesible oportunamente según lo requieran quienes estén autorizados para acceder a ellos.

2.5. Encargado: Persona a cargo de velar por el cumplimiento de esta Política y cumplir las demás obligaciones que esta establece.

2.6. Evento de seguridad de la información: Ocurrencia de un estado o situación que configura o sugiere un incumplimiento actual o posible de la política de seguridad de la información, o una falla de los controles de seguridad.

2.7. Incidente de seguridad de la información: Uno o más eventos de seguridad de la información inesperados o no deseados que, en forma cierta o con una probabilidad significativa, comprometen las operaciones de BH Compliance y amenazan la seguridad de los activos de información.

2.8. Integridad: Protección de la exactitud de la información, permitiendo que esta solo pueda ser modificada o eliminada por personas o procesos autorizados.

3. DIRECTRICES GENERALES DE SEGURIDAD DE LA INFORMACIÓN

3.1. ALMACENAMIENTO DE LA INFORMACIÓN

Los activos de información deberán almacenarse en los repositorios que tenga al efecto BH Compliance, sea *on premise* o en la nube. Se privilegiará contar con repositorios centralizados, siempre que ello sea necesario y factible en conformidad con el funcionamiento y recursos de la compañía.

3.2. CLASIFICACIÓN DE LA INFORMACIÓN

La información en BH Compliance se clasifica de acuerdo con esta tabla.

En caso de no estar seguro si cierta información es confidencial o no, se debe asumir que es confidencial.

Tipo de información	Descripción	Ejemplos
Pública	Esta información está disponible para cualquier persona.	▪ Información que se encuentra disponible en sitios Web ▪ Publicaciones
Interna	Información que puede ser utilizada por todos los trabajadores de BH Compliance. Podría entregarse esta información a terceros, previa autorización de acuerdo con esta Política.	▪ Política de Seguridad ▪ Políticas y/o procedimientos de uso general ▪ Comunicaciones internas
Confidencial	Esta información ha sido revelada a determinadas personas de BH Compliance. Sólo tendrán acceso a la información confidencial quienes necesiten hacerlo en atención a sus funciones, y estén sujetos a obligaciones de confidencialidad. No puede divulgarse a terceros, sino solo previa autorización escrita, específica y de acuerdo con esta Política.	▪ Toda la información de o preparada para los Clientes ▪ Cualquier información que contenga datos personales ▪ Información de Recursos Humanos ▪ Información operacional del negocio de BH Compliance

3.3. ACCESO A LA INFORMACIÓN

El acceso a la información debe ser restringido, siguiendo siempre la clasificación de la información establecida en la sección 3.2.

Los Usuarios no podrán extraer información de los sistemas de BH Compliance, ni guardarla en sus propios dispositivos, a menos tengan la autorización previa y escrita del Encargado y del cliente correspondiente. Obtenida esta autorización, deberán resguardar la información bajo medidas de seguridad necesarias.

Los Usuarios solo podrán entregar información interna o confidencial a terceros en los siguientes casos:

a) Con la autorización previa y escrita del propietario o controlador de la información (p.ej. el cliente);

b) A terceros que requieran la información estrictamente en el contexto de la asesoría para la cual BH Compliance haya sido contratado y para darle curso;

c) A terceros que requieran la información para prestar los servicios que ha contratado BH Compliance, o

d) Existencia de una obligación legal. En este caso, el trabajador deberá contar con la autorización previa de su superior directo.

3.4. USO DE LA INFORMACIÓN

Sin perjuicio del resto de las obligaciones establecidas en esta Política, se deberá cumplir con las siguientes obligaciones al acceder y usar la información de BH Compliance (o de sus Clientes):

a) Los Usuarios deberán velar por la seguridad de la información que manejan, en atención a su clasificación, los requerimientos que permitan resguardar los principios de confidencialidad, integridad y disponibilidad de la información, y los requisitos que establezca la legislación aplicable, especialmente en materias de seguridad de la información y protección de datos personales.

b) Los Usuarios deberán proteger los activos de información del acceso y tratamiento no autorizado y, en general, de la ocurrencia de un incidente de seguridad de la información.

c) Los trabajadores deberán participar en las charlas y capacitaciones sobre seguridad de la información que señale el Encargado o BH Compliance.

d) Los Usuarios deberán respetar la propiedad intelectual e industrial de BH Compliance y sus Clientes.

e) Los Usuarios deberán reportar los incidentes de seguridad al Encargado en conformidad con la sección 3.4. de esta Política.

Terminada la relación laboral o contractual con BH Compliance, según sea el caso, como también en cualquier momento durante el curso de esta relación según sea requerido, y previo a la firma del respectivo finiquito en el caso de los trabajadores, los Usuarios deberán cesar en el uso de todos los activos de información de la compañía y devolver los que se encuentren en su poder, quedando prohibido llevarse o utilizar información de BH Compliance (o sus Clientes). BH Compliance podrá en todo momento remover los accesos y revocar los permisos que se hayan otorgado.

3.5. ADMINISTRACIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad deben ser reportados y gestionados en conformidad a las reglas siguientes:

a) Los Usuarios tienen la obligación de reportar, tan pronto como sea posible, la ocurrencia o sospecha de ocurrencia de cualquier incidente de seguridad de la información, sea o no ocasionado por ellos, al Encargado, a través de los medios que éste defina.

   Además de los incidentes de seguridad que puedan ocurrir dentro de BH Compliance, es necesario estar atentos a aquellos incidentes de seguridad de la información que puedan afectar a los proveedores de BH Compliance, o cualesquiera otros terceros que trabajen para BH Compliance.

b) El Encargado, o quien este designe, deberá gestionar los incidentes de seguridad evaluando y determinando su gravedad con el objeto de activar los mecanismos adecuados de acuerdo con su calificación, y realizar seguimiento de los mecanismos implementados.

Por ejemplo, configuran un incidente de seguridad de la información cualquier divulgación o envío de información a terceros no autorizados, sin importar si tal divulgación es intencional o accidental; cualquier acceso lógico de terceros, conocidos o desconocidos, a información; la pérdida de documentos en soporte físico (papel) o electrónico; robos, daños o pérdidas de los equipos de la oficina, como notebooks y

celulares; o accesos sospechosos o no autorizados a nuestras oficinas que puedan poner en riesgo la seguridad de los activos de información.

4. MEDIDAS DE SEGURIDAD LÓGICA

El acceso de terceros no autorizados a nuestros sistemas puede poner en peligro la información de BH Compliance y de los Clientes. Por tanto, el acceso los sistemas computaciones de BH Compliance estará controlado, entre otras medidas, de la siguiente manera:

a) Todo trabajador tendrá una cuenta de usuario personal con identificador único y contraseña, que actuará como una credencial que lo identifique unívocamente para acceder y usar los recursos de la red corporativa de BH Compliance, los cuales serán personales, confidenciales e intransferibles. En consecuencia, solo el trabajador podrá usar sus credenciales, y será responsable por el mal uso que pueda dársele a su cuenta por terceros no autorizados derivados de su falta de cuidado. En caso de requerirse un uso compartido, debe solicitar autorización al Encargado.

b) Para acceder a los computadores y al escritorio remoto, el trabajador deberá ingresar sus credenciales, según lo señalado en la letra a) anterior, y luego aprobar el ingreso por medio una herramienta de autentificación de dos factores.

c) Las contraseñas deberán seguir las pautas establecidas por BH Compliance.

d) Todo trabajador deberá usar su correo electrónico institucional (@bh-compliance.com) para fines laborales y no para fines personales. El correo electrónico institucional debe utilizarse cuidadosamente, poniendo especial atención a la información enviada y a el/los destinatarios.

e) El acceso a internet usando los sistemas de BH Compliance deberá realizarse dentro de los límites impuestos por la ley, el Reglamento Interno, el Contrato de Trabajo y en todo caso de forma apropiada para el lugar de trabajo.

f) Todo documento elaborado para un cliente o con ocasión del servicio prestado a este, debe quedar registrado y guardado en su carpeta correspondiente (en OneDrive, o en el sistema entonces utilizado por la empresa). Lo anterior permitirá la auditoría y la recuperación de datos, en caso de ser necesario.

5. MEDIDAS DE SEGURIDAD FÍSICAS

El acceso de terceros no autorizados a nuestras dependencias puede poner en peligro la información de BH Compliance y de los Clientes. Por tanto, el acceso físico a las oficinas de BH Compliance estará controlado por las siguientes medidas:

a) Los trabajadores y determinados terceros deben utilizar tarjetas de acceso a las oficinas de BH Compliance.

b) Los terceros autorizados (visitas) deben registrarse en la recepción del edificio.

c) Los trabajadores son responsables de los terceros autorizados (visitas) que se encuentren en las oficinas, por lo que deben preocuparse que éstos no accedan a oficinas o dependencias donde no deberían estar.

d) Los trabajadores deben reportar inmediatamente actividades o personas sospechosas, incidentes y la pérdida de su tarjeta de acceso, enviando un correo a soporte@bh-compliance.com

6. OBLIGACIONES Y PROHIBICIONES ACERCA DEL USO Y RESGUARDO DE EQUIPOS Y RECURSOS DE LA EMPRESA

Sin perjuicio de las obligaciones establecidas en otras secciones de esta Política, los Usuarios deben cumplir con las siguientes obligaciones y prohibiciones respecto al resguardo y protección de los equipos y dispositivos que les hayan sido asignados por BH Compliance, como computadores, *tablets*, o celulares (los "Equipos").

6.1. Obligaciones sobre la seguridad de Equipos

a) Los Usuarios deben emplear el mayor cuidado para proteger los Equipos. En este sentido, los Usuarios deben resguardar físicamente los Equipos, así como la información contenida en ellos. Se deberán tomar todas las medidas razonablemente necesarias para impedir el acceso a terceros no autorizados a la información de BH Compliance y los Clientes.

b) Los Usuarios deben utilizar los Equipos únicamente para el desarrollo de actividades acordes con el desempeño de sus funciones -en el caso de trabajadores- o necesarios para prestar sus servicios -en el caso de proveedores y contratistas-. Excepcionalmente, se podrá usar los Equipos para fines personales, siempre que este uso (i) no interfiera con el desempeño de su trabajo o servicio, (ii) no afecte de otra forma los intereses de BH Compliance, especialmente la seguridad de la información, y (iii) no signifique el almacenamiento de información personal. El uso personal de los Equipos en conformidad a lo señalado será de exclusiva responsabilidad del Usuario que los tenga a su cargo. El uso para fines personales excepcional recién descrito no obstará a la facultad de BH Compliance para borrar o modificar la información contenida en un dispositivo, si ello fuera coherente con sus políticas.

c) Los Usuarios deberán mantener los escritorios y pantallas del computador con el que trabajen o presten servicios -según sea el caso- despejados, con el objeto de prevenir cualquier acceso no autorizado, pérdida o daño de la información.

   En este sentido, los Usuarios:

   i. No deben dejar documentos físicos como papeles en su escritorio o en el lugar en el que se encuentren trabajando o prestando servicios, según sea el caso. Tampoco se debe dejar información de contraseñas, claves de acceso o de otros datos similares a simple vista. Si se ausentan del puesto de trabajo o lugar en el que prestan los servicios y no pueden guardarlos, deberán invertirlos para que no quede a simple vista de los demás.

   ii. Al ausentarse de su escritorio o del lugar donde se encuentren trabajando o prestando servicios, deben guardar toda la información y bloquear su computador o apagarlo.

d) En caso de pérdida de algún dispositivo móvil o equipo, los Usuarios deben reportarlo inmediatamente enviando un mail al Encargado.

Las reglas establecidas en las letras a), b) y c), serán aplicables respecto de los equipos de propiedad del *trabajador* que hayan sido excepcionalmente autorizados por BH Compliance para ser usados con fines laborales.

6.2. Prohibiciones sobre el uso de los equipos

a) Está prohibido deshabilitar mecanismos de control de acceso, software antivirus o cualquier otro componente de seguridad de los equipos que le haya asignado BH Compliance.

b) Está prohibido descargar o instalar software en los equipos que le haya asignado BH Compliance. En caso de necesitar instalar un software necesario para el desempeño de sus funciones, deberán contactar a soporte@bh-compliance.com

c) Está prohibido usar los equipos que le haya asignado BH Compliance para involucrarse en actividades que signifiquen la invasión de la privacidad de un tercero, o que creen un ambiente de trabajo hostil.

d) Está prohibido usar el correo electrónico institucional para suscribirse a servicios no relacionados con el trabajo, redes sociales, realizar compras por internet, y realizar reclamos de carácter personal, entre otros.

Las reglas señaladas en las letras a), c) y d) serán aplicables respecto de los equipos de propiedad del *trabajador* que hayan excepcionalmente sido autorizados por BH Compliance para ser usados con fines laborales.

7. PROPIEDAD INTELECTUAL

7.1. Regla general

Cualquier acceso a la información y material de otras compañías o personas deberá respetar sus derechos de propiedad intelectual, y no se podrá copiar, modificar o reenviar sin la autorización previa y por escrito del titular de tales derechos.

7.2. Software

Descargar/instalar software "pirata" o no licenciado en los equipos de o proporcionados por BH Compliance crea un riesgo de ciberseguridad y responsabilidad legal para BH Compliance. En consecuencia, bajo ninguna circunstancia los Usuarios podrán descargar/instalar este tipo de software.

8. CUMPLIMIENTO

Todos los Usuarios deberán cumplir esta Política, así como las normas, procedimientos y cualquier documento que se pueda dictar al efecto.

Un incidente de seguridad de la información puede constituir en ciertos casos un delito sancionado por la ley Nº 19.223 que tipifica figuras penales relativas a la informática. El acceso no autorizado a datos personales (entendiendo por datos personales cualquier información relativa a una persona natural identificada o identificable) configura un incumplimiento a la ley Nº 19.628 sobre Protección de la Vida

Privada, que obliga a las personas que trabajan con Datos Personales a guardar secreto de ellos.

Los Usuarios tienen la obligación de informar al Encargado del incumplimiento de las obligaciones emanadas de esta Política del que tomen conocimiento, quien tomará en consideración la particularidad de cada situación y adoptará las medidas adecuadas y pertinentes que corresponda.

Cualquier infracción a esta Política, y a los procedimientos o normas que deriven de ella, por parte de un trabajador de BH Compliance, podrá dar lugar a medidas disciplinarias en contra del infractor de acuerdo con lo establecido en el Reglamento Interno de BH Compliance.

En conformidad con lo establecido en el Reglamento Interno y los contratos de trabajo, BH Compliance podrá monitorear y analizar el uso de los sistemas informáticos incluyendo examinar el uso de las tecnologías de la información y comunicación de BH Compliance que se consideren relevantes para evaluar el cumplimento de la Política.

9. VIGENCIA

Las disposiciones de esta Política entrarán en vigencia en un plazo de tres meses desde su aprobación.

10. REVISIÓN Y CONTROL

El cumplimiento de esta Política deberá ser evaluado y supervisado periódicamente. Esta supervisión será responsabilidad del Encargado o quien este le encomiende.

La Política será revisada y actualizada anualmente por el Encargado con el propósito de asegurar su adecuación ante cambios relevantes en materia legislativa, organizacional, tecnológica o derivados de obligaciones contractuales contraídas por BH Compliance, que puedan influir en ella, permitiendo de esta manera una mejora continua y periódica de la misma.

11. CONSULTAS

La Política la podrán encontrar en la intranet y además se distribuirá a todos los trabajadores de BH Compliance.

Ante cualquier duda, sospecha o verificación de incumplimiento de esta Política, se deberá informar a la brevedad posible al Encargado, quien le entregará la ayuda necesaria para manejar el asunto adecuadamente.