

Manual de Manejo e Intercambio de Información para Consultores de BlatoRH Group



Control de Cambios de Documento

Cualquier modificación o cambio al presente Documento se deberá reflejar a continuación:

Versión:	1.0	Fecha:	01/08/2024
Responsable:	Angeles Simal / Pablo Bascoy	Revisado por:	Francisco Torres
Motivo:	Confección inicial del documento		
Versión:		Fecha:	
Responsable:		Revisado por:	
Motivo:			

Compromiso de Confidencialidad

El presente documento es de propiedad intelectual de BlatoRH Group, en adelante la **Consultora** o **BlatoRH**, y proporciona al **Destinatario** (Cliente, Consultor, u otro que lo reciba), con carácter de confidencial.

Este documento no podrá ser copiado bajo ninguna circunstancia, de manera total o parcial a excepción de que la Consultora proporcione por escrito la respectiva autorización.

El Destinatario como la Consultora utilizaran este documento para dejar constancia y en conocimiento del Destinatario, respecto de las políticas y procedimientos de BlatoRH.

El Cliente al recibir este documento, acepta y asume la obligación de respetar la presente cláusula de confidencialidad y respeto de la propiedad intelectual.

La Consultora y el Destinatario se comprometen a no divulgar la información que se encuentre en este documento.

Alcance

1. Almacenamiento de Información

- ☐ Los consultores deben almacenar la información en los **servidores en la nube de Google** de BlatoRH Group.
- ☐ La información debe organizarse en **carpetas por temas**, donde el propietario de la carpeta decide si es de **uso común** dentro del ecosistema BlatoRH o de **acceso restringido** a ciertos miembros.
- ☐ **No se requiere** que la información almacenada esté encriptada.
- ☐ Se sugiere **clasificar la información** en tres categorías:
 - **Pública:** Información accesible por cualquier persona dentro y fuera de la organización sin restricciones.
 - **Interna:** Información destinada únicamente para uso interno de BlatoRH Group y sus consultores.
 - **Confidencial:** Información altamente sensible que debe ser protegida y accesible sólo por personas autorizadas.

2. Intercambio de Información

- ☐ Los medios aprobados para compartir información son las **herramientas de la suite de Google**, incluyendo Google Drive, Docs, Sheets y Slides. como también herramientas homologadas por BlatoRH Group por ejemplo Excel, powerpoint, Word, etc
- ☐ La información **solo debe compartirse con clientes aprobados y no con otros consultores** que no trabajen para BlatoRH Group.
- ☐ Para compartir información **clasificada como Confidencial**, se deben seguir estas medidas adicionales:
 - Utilizar **autenticación adicional**, asegurando que solo las personas autorizadas tengan acceso.
 - Verificar los **permisos de acceso** antes de compartir documentos o archivos.
 - Evitar compartir enlaces públicos; en su lugar, compartir directamente con cuentas específicas mediante invitaciones.

3. Acceso y Control de Información

- ☐ La información clasificada como **Confidencial** debe ser accesible únicamente por los **socios de BlatoRH Group** y las personas que ellos designen.
- ☐ Durante el proceso de **offboarding**, se lleva a cabo:
 - **Revocar inmediatamente** todos los accesos a la información y sistemas de la empresa.

- Asegurar que el consultor **no retiene copias** de información confidencial en dispositivos personales.

4. Uso de Información en Dispositivos Móviles

- ☐ **No se permite acceder** a la información clasificada como **Confidencial** desde dispositivos móviles, para minimizar el riesgo de pérdida o fuga de datos.
- ☐ El acceso a información **Pública e Interna** desde dispositivos móviles está permitido, siempre y cuando:
 - El dispositivo cuente con **medidas de seguridad básicas**, como bloqueo de pantalla y actualización regular del sistema operativo.
 - Se evite el uso de **redes Wi-Fi públicas** no seguras al acceder a información sensible.

5. Backup y Recuperación de Datos

- ☐ Las políticas de backup son las **propias de Google**, que realiza **copias de seguridad automáticas** de la información almacenada en sus servidores.
- ☐ No se requieren **acciones adicionales** por parte de los consultores para el respaldo de la información.
- En caso de pérdida o corrupción de datos, se debe:
 - Contactar al **equipo de soporte de TI** de BlatoRH Group para iniciar el proceso de recuperación.
 - **No intentar restaurar** datos de fuentes no autorizadas que puedan comprometer la integridad de la información.

6. Manejo de Información en Caso de Incidentes

- ☐ En caso de una **fuga de datos** o **acceso no autorizado** a la información, los consultores deben:
 - **Notificar inmediatamente** a su supervisor directo y al **equipo de seguridad de la información** de BlatoRH Group.
 - Proporcionar **detalles completos** del incidente, incluyendo la naturaleza de la información comprometida y las circunstancias del suceso.
- ☐ Se deben seguir los **procedimientos internos establecidos** para:
 - **Contener y mitigar** el impacto del incidente.
 - **Documentar** el incidente para futuras referencias y mejoras en las políticas de seguridad.
 - **Notificar** a las partes afectadas si es necesario y conforme a las regulaciones aplicables.

7. Eliminación Segura de Información

- ☐ Para la **eliminación segura** de información confidencial, se recomienda utilizar las **herramientas de eliminación permanente** proporcionadas por Google.
- ☐ Al eliminar **medios físicos** (como discos duros), se debe:
 - Utilizar **técnicas de destrucción certificadas**, asegurando que la información **no pueda ser recuperada**.
 - Documentar el proceso de destrucción, incluyendo **fechas y métodos utilizados**, para mantener un registro adecuado.
- ☐ Se debe **evitar** el uso de **métodos inseguros** o no certificados que puedan permitir la recuperación de información sensible.

8. Formación y Concienciación

Los consultores reciben anualmente jornada de concientización sobre el manejo seguro de la información, incluyendo:

- ☐ Mejores prácticas para el almacenamiento y compartición de datos.
- ☐ Actualizaciones sobre nuevas amenazas y cómo mitigarlas.
- ☐ Procedimientos a seguir en caso de incidentes de seguridad.


Según sea conveniente la formación puede incluir:

- ☐ Talleres presenciales o virtuales.
- ☐ Cursos en línea y seminarios web.
- ☐ Boletines informativos y materiales de lectura.
- ☐ Evaluaciones de verificación de conocimiento de los consultores sobre las políticas de manejo de información.
- ☐ Feedback y retroalimentación continua para mejorar y actualizar las políticas según sea necesario.

Conformidad

A continuación se deja constancia de la Conformidad de BlatoRH y el Destinatario, en relación a lo especificado en el presente Documento.

Por BlatoRH Group

Firma	
Aclaración	Leonardo Blau
Puesto/Cargo	Director
Fecha	01/08/2024

Por Destinatario

Firma	
Aclaración	
Empresa	
Puesto/Cargo	
Fecha	

