# Política de Seguridad de la Información

**CÓDIGO: IT-POL-0002**

| Nº Revisión | Realizado por | Aprobado por |
|---|---|---|
| **00** | **Responsable del SGSI** | Firmado por ***1388** GUILLERMO |

Soluciones 360°
DIGITAL | FLEXIBLE | GLOBAL

# Contenido

# Control de Revisiones

| Revisión | Fecha | Descripción del cambio |
|---|---|---|
| 00 | 24/11/2025 | Versión inicial. Implantación. |
| 001 | 29/12/2025 | Se incluye a los requerimientos de la ISO27001. |

# 1. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información es efectiva desde la fecha de firma y hasta que sea reemplazada por una nueva Política.

# 2. Misión de la organización

VB GLOBAL GROUP SL es una compañía especializada en la gestión integral de viajes y soluciones de movilidad, con un enfoque prioritario en el segmento corporativo. Nuestro equipo de profesionales combina experiencia, servicio personalizado y tecnología para transformar la forma en que las empresas y los viajeros gestionan sus desplazamientos.

A través de nuestras diferentes marcas ofrecemos soluciones innovadoras y sostenibles que abarcan viajes corporativos, servicios turísticos y experiencias adaptadas a las necesidades de cada cliente.

Nuestro objetivo es ser el socio estratégico de confianza que acompaña a empresas y viajeros, optimizando recursos, mejorando la experiencia de viaje y aportando valor en cada proyecto.

Para alcanzar esta meta, VB GLOBAL GROUP SL asume su compromiso con la seguridad de la información, garantizando la adecuada gestión de esta con respecto a los requisitos establecidos en las normas de referencia ISO/IEC 27001:2022 y RD 311/2022 (ENS), con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes. En línea con el artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación), los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

A tal efecto, los sistemas en VB GLOBAL GROUP SL deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

De igual modo, los sistemas TIC deben estar protegidos frente a amenazas de rápida evolución que puedan incidir negativamente en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas y garantizar la prestación continua de los servicios, es imprescindible contar con una estrategia que se adapte a los cambios en las condiciones del entorno. En este sentido, los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el ENS, así como llevar a cabo un seguimiento continuo de los niveles de prestación de servicios, supervisar y analizar las vulnerabilidades reportadas, y establecer procedimientos de respuesta ante incidentes.

Asimismo, será de obligado cumplimiento para todo el personal y terceros que, en el ejercicio de sus funciones, tengan acceso a la información o a los sistemas mencionados.

## 3. Alcance

Esta Política se aplica a todos los sistemas de información que soportan los servicios de gestión integral de viajes corporativos y particulares, incluyendo la gestión de viajes de empresa, viajes de negocios, congresos, incentivos y servicios MICE, así como a la información tratada en cualquier formato.

## 4. Objetivos

Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información:

- Proporcionar un marco para aumentar la capacidad de resistencia o resiliencia para dar una respuesta eficaz.
- Asegurar la recuperación rápida y eficiente de los servicios frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.
- Prevenir incidentes de seguridad de la información, en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.
- Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

## 5. Marco Normativo

Uno de los objetivos de VB GLOBAL GROUP SL consiste en garantizar el cumplimiento de los requisitos legales aplicables y de cualesquiera otros requisitos suscritos, incluidos los compromisos adquiridos con los clientes, así como la actualización continua de los mismos.

A tal fin, el marco legal y regulatorio en el que la entidad desarrolla sus actividades es el siguiente:

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en lo que no se oponga al Reglamento (UE) 2016/679 y a la Ley Orgánica 3/2018.

- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI).
- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.
- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.
- ISO/IEC 27001:2022 marco del Sistema de Gestión de Seguridad de la Información.

## 6. Desarrollo

Para poder lograr estos objetivos es necesario:

- Mejorar continuamente el sistema de seguridad de la información.
- Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, en caso de materializarse, puedan causar.
- Preservar los intereses de las principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.
- Trabajar de forma conjunta con los proveedores con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de la actividad.
- Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de los procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.
- Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.
- Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.
- Estructurar el sistema de gestión de forma que sea fácil de comprender. El sistema de gestión de VB GLOBAL GROUP SL tiene la siguiente estructura:


La gestión del sistema en VB GLOBAL GROUP SL se encomienda al Responsable de Sistemas Informáticos y estará disponible en un repositorio integrado en el sistema de información de la empresa, al que se podrá acceder de acuerdo con los perfiles de acceso concedidos conforme al procedimiento vigente de gestión de los accesos.

La documentación referida a la seguridad del sistema se encuentra estructurada en carpetas dentro del entorno SharePoint de VB Global Group (All in One), dividido en subcarpetas nombradas por puntos de norma y marcos de operación. Dichas subcarpetas recogen los distintos procedimientos, registros y evidencias, y su acceso está restringido al personal de la compañía, no permitiéndose el acceso a personal externo no autorizado.

La documentación de seguridad se estructura en:

- Política de Seguridad.
- Normativa de seguridad: documentos que describen el uso de equipos, servicios e instalaciones. Describen lo que se considera uso indebido, la responsabilidad del personal con respecto al cumplimiento o violación de la normativa, derechos, deberes y medidas disciplinarias de acuerdo con la legislación vigente.
- Documentos específicos: documentación de seguridad desarrollada según las guías CCN-STIC que resulten de aplicación.
- Procedimientos de seguridad: documentos que detallan cómo operar los elementos del sistema.

Esta política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar el sistema de gestión de la entidad.

## 7. Organización de seguridad

La responsabilidad esencial recae sobre la Dirección General de la organización, que debe organizar las funciones y responsabilidades, así como facilitar los recursos adecuados para alcanzar los objetivos del ENS. Los directivos son también responsables de dar buen ejemplo siguiendo las normas de seguridad establecidas.

Estos principios son asumidos por la Dirección, quien dispone los medios necesarios y dota a los empleados de los recursos suficientes para su cumplimiento, plasmándose y poniéndolos en público conocimiento a través de la presente Política de Seguridad.

Los roles o funciones de seguridad definidos son:

| Función | Deberes y responsabilidades |
| --- | --- |
| **Responsable de la información (RINFO)** | ▪ Tomar las decisiones relativas a la información tratada. |
| **Responsable de los servicios (RSER)** | ▪ Coordinar la implantación del sistema.<br>▪ Mejorar el sistema de forma continua. |
| **Responsable de la seguridad (RSEG o CISO)** | ▪ Determinar la idoneidad de las medidas técnicas.<br>▪ Proporcionar la mejor tecnología para el servicio. |
| **Responsable del sistema (RSIS)** | ▪ Coordinar la implantación del sistema.<br>▪ Mejorar el sistema de forma continua. |
| **Dirección** | ▪ Proporcionar los recursos necesarios para el sistema.<br>▪ Liderar el sistema. |

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en los documentos del sistema (Acta del Comité de Seguridad).

**RESOLUCIÓN DE CONFLICTOS**
Las diferencias de criterios que pudiesen derivar en un conflicto se tratarán en el seno del Comité de Seguridad y prevalecerá en todo caso el criterio de la Dirección General.

## 8. Comité de Seguridad

El procedimiento para su designación y renovación será la ratificación en el Comité de seguridad.

El comité para la gestión y coordinación de la seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información, de forma que las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité.

Los miembros del comité de seguridad de la información son:

- **RESPONSABLE DE SEGURIDAD:** Jorge Romero Villarreal
- **RESPONSABLE DEL SISTEMA:** Enrique Calzado Salcedo
- **RESPONSABLE DEL SERVICIO:** Jaime Arciénega Poppe
- **RESPONSABLE DE INFORMACIÓN:** Jaime Arciénega Poppe

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones, cuya actividad no queda subordinada a ningún otro elemento de la empresa.

La organización de la Seguridad de la información se desarrolla en la Normativa de Seguridad.

Esta política se complementa con el resto de las políticas, procedimientos y documentos en vigor para desarrollar el sistema de gestión de la entidad.

# 9. Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos en el que se evalúen las amenazas y los riesgos a los que están expuestos.

Este análisis se revisa regularmente:

- al menos una vez al año;
- cuando cambie la información manejada;
- cuando cambien los servicios prestados;
- cuando ocurra un incidente grave de seguridad;
- cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos desarrollada en el procedimiento Análisis de Riesgos.

# 10. Gestión de Personal

Todos los miembros de VB GLOBAL GROUP SL tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad TIC disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de VB GLOBAL GROUP SL atenderán a una sesión de concienciación en materia de seguridad de IT al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de VB GLOBAL GROUP SL, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto en la primera asignación como en cambios de puesto de trabajo o de responsabilidades en el mismo.

# 11. Profesionalidad y seguridad de los recursos humanos

Esta política se aplica a todo el personal de VB GLOBAL GROUP SL y al personal externo que realice tareas dentro de la empresa.

Personas & Valores incluirá funciones de seguridad de la información en las descripciones de los trabajos de los empleados; informará a todo el personal de nuevo ingreso de sus obligaciones con respecto al cumplimiento de la Política de Seguridad de la Información; gestionará los Compromisos de Confidencialidad con el personal; y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

- El Responsable de Gestión de la Seguridad (RGS) [CISO] es responsable de monitorear, documentar y analizar los incidentes de seguridad reportados, así como de comunicarlos al Comité de Seguridad de la Información y a los propietarios de información.

- El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Gestión de la Seguridad (RGS) [CISO] gestione los informes de incidentes y anomalías del sistema. Asimismo, el Comité estará informado de los incidentes, supervisará su investigación y evolución, y promoverá su adecuada resolución.

- El Responsable de Gestión de la Seguridad (RGS) [CISO] participará en la preparación del Compromiso de Confidencialidad que deberán firmar los empleados y terceros que desempeñen funciones en VB GLOBAL GROUP SL, así como en el asesoramiento sobre las sanciones aplicables por el incumplimiento de esta Política y en el tratamiento de los incidentes de seguridad de la información.

- Todo el personal de VB GLOBAL GROUP SL es responsable de informar de manera oportuna sobre las debilidades e incidentes de seguridad de la información que detecten.

- Profesionalidad de los recursos humanos:

    - Determinar la competencia necesaria del personal para el desempeño de las funciones que afectan a la Seguridad de la Información.
    - Asegurar que el personal sea competente, sobre la base de la educación, capacitación o experiencia adecuadas.
    - Mantener la información documentada necesaria para demostrar la competencia del personal en materia de Seguridad de la Información.

Los objetivos del control de la seguridad del personal son:

- Reducir los riesgos derivados del error humano, la puesta en marcha de irregularidades, el uso indebido de instalaciones y los recursos, y manejo no autorizado de la información.

- Explicar las responsabilidades en materia de seguridad de la información durante la etapa de reclutamiento del personal, incluirlas en los acuerdos que se deban firmar y verificar su cumplimiento durante el desempeño de las tareas asignadas al empleado.

- Asegurarse de que los usuarios conozcan las amenazas y riesgos asociados a la seguridad de la información, y de que estén adecuadamente capacitados para apoyar el cumplimiento de la Política de Seguridad de la Información en el desarrollo de sus tareas habituales.

- Establecer compromisos de confidencialidad con todo el personal y usuarios fuera de las instalaciones de procesamiento de información.

- Implementar las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad y de los incidentes existentes, con el fin de minimizar su impacto y prevenir su reincidencia.

# 12. Autorización y control de acceso a los Sistemas de Información

El control del acceso a los sistemas de información tiene por objetivo:

- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de VB GLOBAL GROUP SL y otras redes públicas o privadas.
- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

# 13. Protección de las instalaciones

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, así como los daños e interferencias, a la sede, las instalaciones y la información de VB GLOBAL GROUP SL.
- Proteger el equipo de procesamiento de información crítico de VB GLOBAL GROUP SL, ubicándolo en áreas protegidas, delimitadas por un perímetro de seguridad definido, y dotadas de las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección del equipo durante su traslado y cuando deba permanecer fuera de las áreas protegidas por motivos de mantenimiento u otras causas.
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipo de cómputo que alberga la información de VB GLOBAL GROUP SL.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el desarrollo normal de sus tareas habituales.
- Proporcionar una protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de VB GLOBAL GROUP SL: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

El responsable de Gestión de la Seguridad (RGS) [CISO], junto con los Titulares de la Información cuando proceda, definirá las medidas de seguridad física y ambiental necesarias para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. Asimismo, verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

Los responsables de los distintos departamentos definirán los niveles de acceso físico del personal de VB GLOBAL GROUP SL a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizarán formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de VB GLOBAL GROUP SL cuando lo consideren apropiado.

Todo el personal de VB GLOBAL GROUP SL es responsable del cumplimiento de la política de pantalla y escritorio limpios, con el fin de proteger la información relacionada con el trabajo diario en las oficinas.

## 14. Adquisición de productos

Los distintos departamentos deberán cerciorarse de que la seguridad TIC forme parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, incluidas las decisiones de desarrollo o adquisición y las actividades de explotación.

Los requisitos de seguridad y las necesidades de financiación deberán identificarse e incluirse en la planificación, en la solicitud de ofertas y en los pliegos de licitación para proyectos de TIC.

Por otro lado, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.

La política de desarrollo y adquisición de sistemas de información se desarrolla en el documento “Política Adquisición, Desarrollo y Mantenimiento de Sistemas”.

## 15. Seguridad por defecto

VB GLOBAL GROUP SL considera estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida.

Los sistemas de información y los servicios deberán incluir la seguridad por defecto desde su creación hasta su retirada, incluyendo la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación, de forma que se establezca la seguridad como un proceso integral y transversal.

## 16. Integridad y actualización del sistema

VB GLOBAL GROUP SL se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos y lógicos mediante la autorización previa a su instalación en el sistema.

Dicha evaluación será realizada principalmente por la dirección de sistemas, que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con la debida diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

## 17. Protección de la información almacenada y en tránsito

VB GLOBAL GROUP SL establece medidas de protección para garantizar la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros.

Tendrán la consideración de entornos inseguros los equipos portátiles, los dispositivos periféricos, los soportes de información y las comunicaciones realizadas a través de redes abiertas o con mecanismos de cifrado débiles.

## 18. Datos de carácter personal

Se trata de datos de carácter personal a los que únicamente tendrán acceso las personas autorizadas. Se recogerán los ficheros afectados y los responsables correspondientes.

Todos los sistemas de información de VB GLOBAL GROUP SL se ajustarán a los niveles de seguridad exigidos por la normativa para la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

## 19. Terceras Partes

Cuando VB GLOBAL GROUP SL preste servicios a otros organismos o maneje información de terceros, estos serán partícipes de esta Política de Seguridad de la Información. Asimismo, se establecerán canales para el reporte y coordinación entre los respectivos Comités de Seguridad TIC, así como los procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando VB GLOBAL GROUP SL utilice servicios de terceros o ceda información a estos, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información, quedando sujetos a las obligaciones en estas establecidas. Las terceras partes podrán desarrollar sus propios procedimientos operativos para satisfacer dicha normativa. Asimismo, se establecerán procedimientos específicos para el reporte y resolución de incidencias.

Se garantizará que el personal de terceros esté adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de esta Política no pueda ser satisfecho por una tercera parte en los términos indicados anteriormente, se requerirá un informe del Responsable de Seguridad que identifique los riesgos en los que se incurre y la forma de tratarlos. Dicho informe deberá contar con la aprobación de los responsables de la información y de los servicios afectados antes de seguir adelante.

## 20. Prevención de sistemas de información interconectados

VB GLOBAL GROUP SL establece medidas de protección para la Seguridad de la Información, con especial énfasis en la protección del perímetro y, particularmente, cuando se realizan conexiones a redes públicas utilizadas total o principalmente para la prestación de servicios de comunicaciones electrónicas accesibles al público.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas a través de redes, y se controlarán los puntos de unión de dichas conexiones.

## 21. Registros de actividad

VB GLOBAL GROUP SL registrará las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en todo momento a la persona responsable.

Los objetivos principales de la Gestión de Incidentes de Seguridad de la Información son:

- Establecer un sistema de detección y reacción frente a código malicioso.
- Disponer de procedimientos para la gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Asegurar que tales procedimientos contemplen los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, los canales de comunicación con las partes interesadas y el registro de las actuaciones.
- Tal registro se emplea para la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo tras un incidente.
- Reducir los posibles riesgos e impactos derivados del incidente.
- Preservar la integridad de los sistemas en caso de incidente de seguridad.
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma y ejecutar un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

## 22. Continuidad de la actividad

VB GLOBAL GROUP SL, con el objetivo de garantizar la continuidad de sus actividades, implanta medidas para que los sistemas dispongan de copias de seguridad y establece los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

## 23. Mejora continua del proceso de seguridad

VB GLOBAL GROUP SL establece un proceso de mejora continua de la seguridad de la información, aplicando los criterios y la metodología establecida en normas internacionales, tales como ISO/IEC 27001.

## 24. Comunicación

La presente política será comunicada a todo el personal y estará disponible para las partes interesadas pertinentes en el Repositorio documental ALL IN ONE.

## 25. Cumplimiento obligatorio

El incumplimiento de esta política podrá dar lugar a medidas disciplinarias conforme a la legislación vigente.