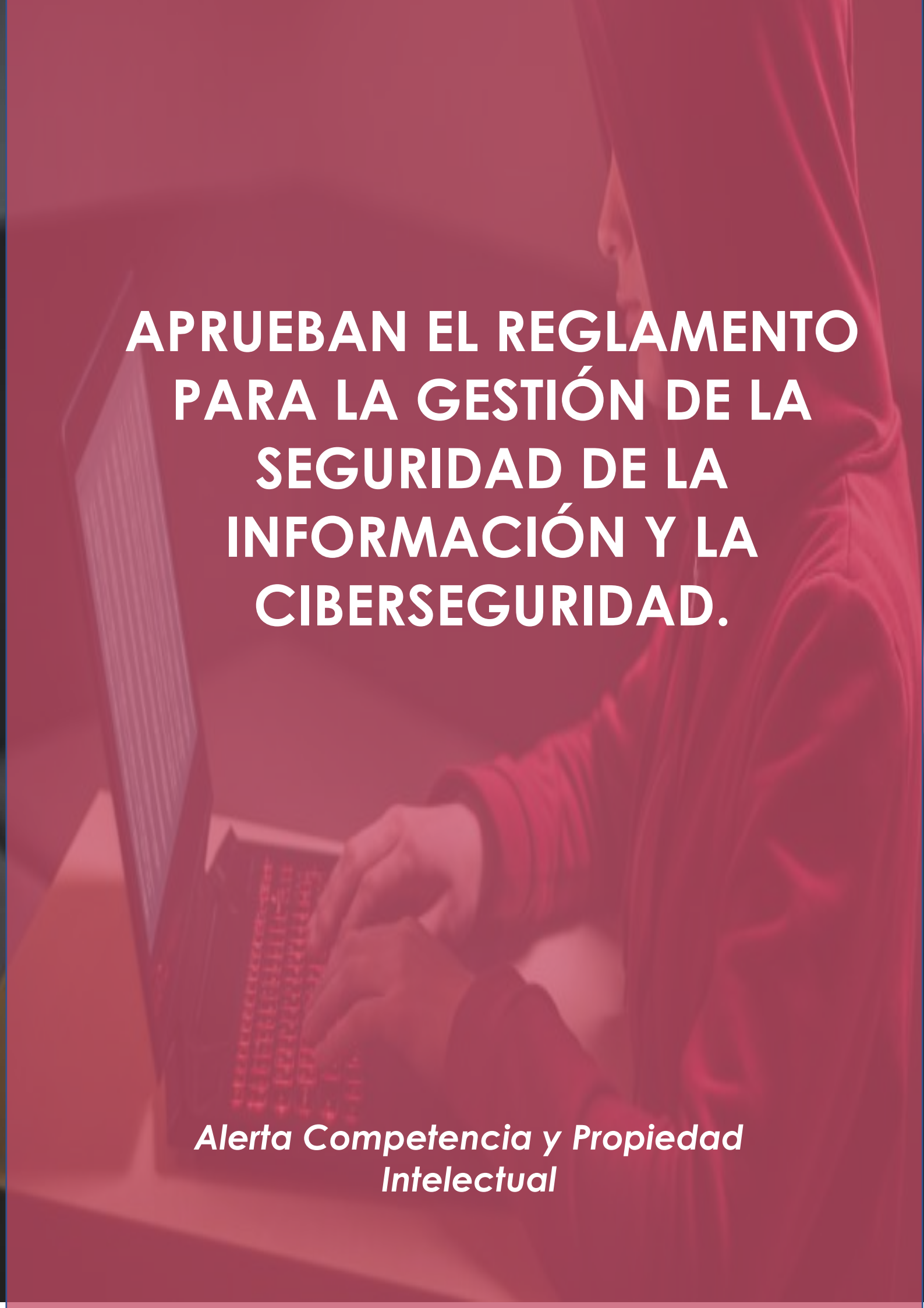

APRUEBAN EL REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD.

Alerta Competencia y Propiedad Intelectual

Benites, Vargas & Ugaz
ABOGADOS

APRUEBAN EL REGLAMENTO PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD

El 23 de febrero de 2021 se publicó en el diario oficial El Peruano, la Resolución SBS N° 504-2021 mediante el cual aprueban el Reglamento para la gestión de la seguridad de la información y la ciberseguridad (en adelante, el Reglamento); y, modifican el Reglamento de Tarjetas de Crédito y Débito.

A continuación, comentaremos los puntos más importantes de la norma:

- **Objeto del Reglamento:** Busca reforzar los sistemas de las empresas del sistema financiero, de seguros y privado de pensiones, en aspectos de ciberseguridad y procesos de autenticación, ante la creciente interconectividad y mayor adopción de canales digitales para la provisión de los servicios.

- **Sobre las definiciones más importantes del Reglamento:**

  - ✓ **Activo de información:** Información o soporte en que ella reside, que es gestionado de acuerdo con las necesidades de negocios y los requerimientos legales, de manera que puede ser entendida, compartida y usada.
  - ✓ **Amenaza:** Evento que pueda perjudicar la operación de las empresas o sus activos de información, mediante el aprovechamiento de una vulnerabilidad.
  - ✓ **Autenticación:** Proceso de verificación de la identidad de una entidad mediante el uso de credenciales que se le asignan.
  - ✓ **Canal digital:** Medio empleado por las empresas para proveer servicios cuyo almacenamiento, procesamiento y transmisión se realiza mediante la representación de datos en bits.
  - ✓ **Ciberseguridad:** Protección de los activos de información mediante la prevención, detección, respuesta y recuperación de los activos de información.
  - ✓ **Incidente:** Evento que tiene un impacto adverso sobre la organización y que requiere de acciones de respuesta y recuperación.
  - ✓ **Vulnerabilidad:** Debilidad que expone a los activos de información ante amenazas que pueden originar incidentes con afectación a los mismos activos de la información.

- **Sobre el sistema de gestión de seguridad de la información y ciberseguridad (SGSI-C):** Es un conjunto de políticas, procesos, roles, procedimientos y responsabilidades para identificar y proteger los activos de información, detectar eventos de seguridad, prever una respuesta ante dichos eventos, y recuperación ante incidentes de ciberseguridad.

Cada programa deberá ser proporcional al tamaño, la naturaleza y la complejidad de sus operaciones.

En esa misma línea, las empresas deberán adoptar las medidas mínimas de seguridad de la información, las cuales conforman el **régimen general** del SGSI-C. Las más relevantes son las siguientes:

Tema	Medidas específicas
Seguridad de los recursos humanos	a) Implementar protocolos de seguridad de la información ante cambios de personal. b) Implementar procesos disciplinarios en caso de incumplimientos de las políticas de seguridad de la información.
Controles de acceso físico y lógico	a) Prevenir accesos no autorizados a la información y a los sistemas. b) Implementar procedimientos de administración de accesos. c) Implementar procesos de autenticación para controlar el acceso a los activos de la información.
Seguridad de las operaciones	a) Asegurar y prever el funcionamiento continuo de las instalaciones de procesamiento, almacenamiento y transmisión de información. b) Mantener la operación de los sistemas informáticos acorde a procedimientos previamente establecidos. c) Controlar los cambios en el ambiente operativo de sistemas, y mantener segregados los ambientes de desarrollo, pruebas y producción. d) Contar con protocolos de respuesta y recuperación ante incidentes de malware; así como generar y probar copias de respaldo de información. e) Contar con una estrategia de respaldo y procedimientos de restauración de información.

Seguridad en las comunicaciones	a) Implementar y mantener la seguridad de redes de comunicaciones acorde a la información que por esta se transmite. b) Asegurar que las redes de comunicaciones y servicios de red son gestionados y controlados para proteger la información. c) Segregar los servicios de información disponibles, usuarios y sistemas en las redes de la empresa. d) Implementar protocolos seguros y controles de seguridad para la transferencia de información tanto interna como externamente de la organización.
Adquisición, desarrollo y mantenimiento de sistemas	a) Implementar y mantener la seguridad en los servicios y sistemas informáticos b) Asegurar que se incluyan prácticas de seguridad de la información en las aplicaciones y sistemas informáticos. c) Asegurar que se efectúen pruebas técnicas, funcionales y de seguridad de la información en los sistemas informáticos.
Gestión de incidencias de ciberseguridad	a) Implementar procedimientos para la gestión de incidentes de ciberseguridad. b) Clasificar los incidentes y prever protocolos de respuesta y recuperación. d)Tener acceso a la información de inteligencia de amenazas, vulnerabilidades e incidentes. e) Implementar reportes internos de ciberseguridad f) Identificar las posibles mejoras para la gestión de incidentes.
Criptografía	a) Utilizarla para asegurar la confidencialidad, autenticidad e integridad de la información.
Gestión de activos de la información	a) Identificar los activos de información mediante inventario y asignarles custodia. b) Establecer medidas para evitar su divulgación.

- **Sobre la responsabilidad del directorio y gerencia de las empresas referidas a la aplicación del SGSI-C:** El directorio es responsable de aprobar y facilitar acciones para contar con un SGSI-C, tal como aprobar políticas y lineamientos para el SGSI-C y su mejora continua; asignar recursos técnicos, de personal y financieros para su implementación; y, aprobar la organización, roles y responsabilidades para el SGSI-C.

Por su parte la gerencia es responsable de tomar las medidas necesarias para implementar el SGSI-G de acuerdo a lo que diga el directorio y el Reglamento, también apoya el buen funcionamiento del SGSI y se encarga de gestionar los riesgos asociados a la seguridad de la información y Ciberseguridad en el marco de sus funciones.

- **Sobre las nuevas funciones del Comité de Riesgos:** Dicho Comité será el encargado de aprobar el plan estratégico del SGSI-C y recomendar acciones a seguir, así como aprobar el plan de capacitación a fin de garantizar el plan de capacitación al personal de la empresa.

  Para ello, será necesario, además, que las empresas constituyan un Comité Especializado en Seguridad de la Información y Ciberseguridad.

- **Sobre el programa de ciberseguridad que las empresas deben implementar:** El Reglamento dispone que toda empresa con presencia en el ciberespacio debe tener un programa de ciberseguridad (PG-C).

  El PG-C deberá prever un diagnostico y plan de mejora sobre las capacidades de ciberseguridad, el cual deberá permitir, por lo menos, lo siguiente:

  - ✓ Identificación de los activos de información.
  - ✓ Protección frente a las amenazas a los activos de información.
  - ✓ Detección de incidentes de ciberseguridad.
  - ✓ Respuesta con medidas que reduzcan el impacto de los incidentes.
  - ✓ Recuperación de las capacidades o servicios tecnológicos que pudieran ser afectados.

- **Sobre el reporte de incidentes de ciberseguridad significativos:** La empresa deberá reportar a la Superintendencia cuando advierta un incidente de ciberseguridad en el cual se presuma o se verifique la pérdida de información de los clientes o la empresa, fraude, interrupción de operaciones, y/o un impacto negativo en la imagen y reputación de la empresa.

  Asimismo, la empresa deberá hacer un análisis forense para determinar las causas del incidente y tomar las medidas para su gestión.

- **Sobre la implementación de procesos de autenticación:** Las empresas deberán implementar procesos de autenticación que permitan controlar el acceso a los servicios que provea a sus usuarios por canales digitales.

  Estos deberán ser reevaluados tras el descubrimiento de vulnerabilidades. Asimismo, las empresas deberán contar con herramientas y procedimientos para el monitoreo de transacciones para evitar operaciones fraudulentas.

- **Sobre las acciones que se deben implementar en los canales digitales utilizados por los usuarios:**

- ✓ El "enrolamiento" o registro de un usuario en servicios provistos por un canal digital deberá verificar la identidad del usuario, con medidas que eviten la suplantación de identidad.

- ✓ De otro lado, se requerirá **la autenticación reforzada** para aquellas acciones que puedan originar operaciones fraudulentas u otro abuso del servicio en perjuicio del cliente. Dichas medidas de autenticación reforzada son las siguientes: usar combinación de factores de autenticación, generar un código de autenticación mediante métodos criptógrafos; y, cuando la operación esa exitosa notificar los datos de la operación al usuario.

  Cabe indicar que dichas acciones reforzadas no serán necesarias cuando se realicen por las siguientes operaciones por canal digital: operaciones de pago, pagos de periódico transferencias a las cuentas de beneficiarios de confianza determinados como tal por el usuario; aquellas realizadas a cuentas en las cuales el beneficiario sea la misma persona; operaciones de pago que representen un nivel de riesgo de fraude bajo, entre otras.

  Sin embargo, cabe indicar que las operaciones no reconocidas por los usuarios que fueron realizadas luego de que el usuario reportara el robo o pérdida de sus credenciales serán responsabilidad de las empresas.

- ❖ **Sobre el régimen simplificado del SGSI-C:** Este requerirá de la planificación y ejecución, por lo menos anual, de las siguientes actividades:

  - ✓ Identificar la información de mayor importancia para la empresa.
  - ✓ Identificar los dispositivos que se conectan a la red interna y todo software que se encuentre instalado en la infraestructura tecnológica.
  - ✓ Identificar cuentas de usuario con permisos de acceso habilitados.
  - ✓ Implementar y mantener una línea base de seguridad en sistemas operativos y aplicaciones utilizadas.
  - ✓ Identificar y evaluar la habilitación de las funciones de seguridad integradas en los sistemas operativos.
  - ✓ Priorizar y gestionar las vulnerabilidades de seguridad identificadas.
  - ✓ Desarrollar una campaña de orientación de adopción de prácticas seguras para los empleados.

- ❖ **Sobre la aplicación de las disposiciones del Reglamento:** Las disposiciones referidas **al régimen general del SGSI-C, ciberseguridad, autenticación y provisión de servicios por terceros especificados** en el Reglamento serán de obligatorio cumplimiento para las siguientes empresas:

  - ✓ Empresa Bancaria;
  - ✓ Empresa Financiera;
  - ✓ Caja Municipal de Ahorro y Crédito - CMAC;
  - ✓ Caja Municipal de Crédito Popular - CMCP;

- ✓ Caja Rural de Ahorro y Crédito - CRAC;
- ✓ Empresa de Seguros y/o Reaseguros
- ✓ Empresa de Transporte, Custodia y Administración de Numerario;
- ✓ Administradora Privada de Fondos de Pensiones;
- ✓ Empresa Emisora de Tarjetas de Crédito y/o de Débito;
- ✓ Empresa Emisora de Dinero Electrónico; y
- ✓ El Banco de la Nación.
- ✓ Las empresas de Seguros y/o Reaseguros cuyo volumen promedio de activos de los últimos tres (3) años sea mayor o igual a 450 millones de soles.

Cabe indicar que en caso las empresas del Sistema Financiero encuentren limitaciones materiales para cumplir con el Régimen General pueden solicitar autorización para la aplicación del Régimen Simplificado del presente Reglamento, para lo cual deberán presentar un informe que sustente la razonabilidad de la solicitud,

Por su parte, **el régimen simplificado** será de obligatoria aplicación para las siguientes entidades:

- ✓ Banco de Inversión;
- ✓ Empresa de Seguros y/o Reaseguros
- ✓ Entidad de Desarrollo a la Pequeña y Micro Empresa – EDPYME;
- ✓ Empresa de Transferencia de Fondos;
- ✓ Derrama y Caja de Beneficios bajo control de la Superintendencia;
- ✓ La Corporación Financiera de Desarrollo –COFIDE;
- ✓ El Fondo MIVIVIENDA S.A.;
- ✓ El Fondo de Garantía para Préstamos a la Pequeña Industria –FOGAPI;
- ✓ El Banco Agropecuario; y,
- ✓ Almacenes Generales.

- ❖ **Sobre el plan de adecuación que deberán presenta las empresas:** En un plazo máximo de sesenta (60) días calendarios las empresas deberán presentar a la Superintendencia un plan de adecuación al Reglamento, la cual deberá incluir un diagnostico preliminar de la situación de la empresa, las acciones previstas para la adecuación total al Reglamento, los funcionarios responsables del cumplimiento del plan, y un cronograma de adecuación.

- ❖ **Sobre la vigencia de la norma:** La norma entra en vigencia el 1 de julio de 2021, excepto la disposición del Reglamento referido a la autorización que se debe solicitar a la Superintendencia para la contratación de un servicio significativo de procesamiento de datos provisto por terceros desde el exterior que entra en vigencia al día siguiente de la publicación del Reglamento.

Para acceder a mayor información, se puede ingresar al siguiente enlace: https://busquedas.elperuano.pe/normaslegales/aprueban-el-reglamento-para-la-gestion-de-la-seguridad-de-la-resolucion-no-504-2021-1929393-1/

Cualquier duda o consulta, nuestros equipos están a su disposición para ampliar sobre el asunto.

Equipo de Competencia y Propiedad Intelectual

Fabricio Sánchez
Jefe de área de competencia y Propiedad Intelectual
fsanchez@bvu.pe

John- André Flores
Abogado Asociado
jfloresu@bvu.pe

Alexandra Espinoza
Asistente
aespinoza@bvu.pe

Av. 28 de Julio 1044 Lima 18 – Perú / Teléfono: (511) 615-9090 / Fax: (511) 615-9091
Calle Fray Bartolomé de las Casas 478, Urb. San Andrés, Trujillo / Teléfono: (044) 60-8866/ Fax: (044) 60-8867 Jr. Robles Arnao 1055 – Urbanización San Francisco, Huaraz / Telefax: (043) 72-4408