Vigencia: 02/02/2015 **Versión: 01**

Elaborado por: Gerente de Gestión de Sistemas
Revisado por: Gerencia General
Aprobado por: Gerente de Consultoría Interna

POLÍTICA CORPORATIVA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETIVO

Establecer la política corporativa de seguridad de la información con la finalidad de proteger la información de ALICORP S.A.A. y subsidiarias a nivel regional asegurando su confidencialidad, disponibilidad e integridad, para minimizar los riesgos y garantizar la continuidad de sus operaciones.

2. ALCANCE

Todos los Colaboradores, miembros de directorio y terceros que, en el marco de un contrato de trabajo, periodo de práctica o prestación de servicios, acceden a la información, sistemas de información y servicios informáticos de ALICORP S.A.A. y subsidiarias a nivel regional.

3. DOCUMENTOS RELACIONADOS:

No aplica

4. RESPONSABILIDADES

Las responsabilidades sobre la ejecución de ésta política son las siguientes:

Responsable	Actividad
Área usuaria:	a. Cumplir con lo dispuesto en la presente política, así como comunicar a los Terceros a su cargo la existencia de la misma. b. Hacer uso responsable de los equipos y servicios informáticos asignados por ALICORP. c. Reportar a mesa de ayuda cualquier incidente de seguridad de la información que involucre a los equipos de cómputo o servicios informáticos.
Área de Gestión de Sistemas de Alicorp	a. Difundir e implementar efectivamente ésta política en todo Alicorp S.A.A. y subsidiarias a nivel regional.
Sistemas Grupo Romero:	a. Aplicar los controles de seguridad que sean necesarios para salvaguardar la información contenida en los equipos de cómputo, así como aquella que se transmite a través de los servicios informáticos. b. Proveer oportunamente los equipos de cómputo una vez que estos son asignados a los colaboradores, así como gestionar los accesos correspondientes a los servicios informáticos autorizados.

5. POLÍTICA GENERAL

La información de ALICORP en cualquiera de sus formas: audio, video, escrito, digital, entre otras, es un activo importante para la continuidad de sus operaciones, por ello ha establecido la siguiente Política de Seguridad de la Información, la cual representa su visión en cuanto a la protección de sus activos de Información:

5.1. Protección de la información

a. Los Colaboradben proteger y hacer uso responsable de la información de ALICORP.
b. Toda la información generada por el colaborador durante su vínculo laboral o contractual es de propiedad

exclusiva de ALICORP, y no debe ser utilizada para fines ajenos al negocio. Por lo que la e mpresa puede ejecutar procesos de auditoria, supervisión y control como parte de su gestión permanente.

c. La divulgación, copia y transferencia de la información confidencial y/o privilegiada debe ser autorizada previamente por el autorizador según sea el caso.
d. Toda la información digital de ALICORP, debe almacenarse en el Servidor de Archivos (Unidad P y carpeta virtual) a fin de garantizar su respaldo.
e. El acceso a la información de ALICORP por parte de Terceros será restringido, asimismo están en la obligación de cumplir con la presente política.

5.2. Recursos asignados

a. Los equipos de cómputo, dispositivos móviles, sistemas de información y servicios informáticos (correo electrónico, internet, intranet, etc.) asignados solo deben ser utilizados para fines laborales, puesto que contienen información y registros de propiedad de Alicorp.
b. Los colaboradores son responsables del cuidado del equipo de cómputo y dispositivo móvil asignado.
c. Solo está permitido la instalación de software licenciado en los equipos de cómputo otorgados por ALICORP que contrata al colaborador. En caso se requiera la instalación de freeware y/o shareware, éste deberá ser validado con el Jefe inmediato y coordinado con la Mesa de Ayuda para la instalación respectiva.
d. Todo equipo de cómputo asignado a los Colaboradores está protegido a través del antimalware corporativo, por lo que de comprobarse un incidente de infección del mismo, este será desconectado de la red corporativa para salvaguardarla. Para el caso de los equipos que sean propios de Terceros se tomarán las mismas acciones de mitigación.
e. Se restringe la conexión de equipos de cómputo y dispositivos móviles personales a la red corporativa.

5.3. Cuenta de usuario asignada

a. El usuario otorgado a cada Colaborador para acceder a los equipos de cómputo, sistemas de información y servicios informáticos lo identifican dentro de la red corporativa, por lo que será responsable de todas las actividades que se realicen con la misma.
b. Los colaboradores no deben compartir sus contraseñas de usuario, asimismo esta debe ser cambiada periódicamente o cada vez que los sistemas de información o servicios informáticos a los que accede se lo soliciten.
c. Todo Colaborador debe bloquear su Equipo de Cómputo asignado al ausentarse o retirarse de su lugar de trabajo.

6. POLÍTICA DE USO ACEPTABLE DE EQUIPOS Y SERVICIOS INFORMÁTICOS:

6.1. Uso de los equipos y servicios informáticos en general

a. Estará justificado en los siguientes casos:
b. Por tareas relacionadas a las funciones asignadas a un colaborador o tercero.
c. Por alguna necesidad de negocio de ALICORP debidamente aprobada por el autorizador.
d. Por fines laborales, de investigación, de administración y de atención al cliente.
e. Deben estar restringidos para los colaboradores en casos de cese.
f. Solo se debe instalar software licenciado en los equipos de cómputo otorgados por ALICORP que contrata al colaborador, esto con la finalidad de no fomentar la piratería informática u otras actividades ilegales relacionadas. En caso se requiera la instalación de freeware y/o shareware, éste deberá ser validado con el Jefe inmediato y coordinado con Mesa de Ayuda para su instalación respectiva.
g. La información de ALICORP, almacenada en los equipos de cómputo, así como aquella que se genera a través del uso de los servicios informáticos es de propiedad exclusiva de ALICORP que contrata al colaborador, por lo que al acceder a la misma son responsables por su tratamiento adecuado.
h. El uso de los equipos de cómputo y servicios informáticos es para fines laborales, por lo que los colaboradores deben evitar realizar acciones que puedan comprometer la integridad, confidencialidad y disponibilidad de la información.
i. La transferencia de archivos en horarios de trabajo mediante el uso de la red corporativa o al internet a través del correo, file servers internos o públicos debe ser utilizado con criterio ya que puede afectar los recursos de red de ALICORP.
j. Los Terceros que acceden a equipos de cómputo y servicios informáticos de ALICORP, están en la obligación de cumplir con la presente política.

6.2. Uso de usuario y contraseñas

a. Todo Usuario y accesos a los servicios informáticos que requiera un Colaborador que labora en ALICORP, deben ser definidos y aprobados por el Autorizador correspondiente, quien debe indicar si son permanentes o temporales.
b. Toda solicitud de acceso debe ser canalizada a través de la Mesa de Ayuda.
c. Los Usuarios son asignados para uso exclusivo del Colaborador a quien se le otorgó, por tanto no deben ser compartidos. Asimismo, son responsables del uso adecuado del Usuario asignado, así como de guardar reserva de sus contraseñas.
d. Los Colaboradores deben cambiar sus contraseñas de Usuario periódicamente o cada vez que los servicios informáticos a los que accede se lo solicite.
e. El área de Recursos Humanos (RRHH) será responsable de tramitar la cancelación y baja de los Usuarios correspondientes a Colaboradores cesados en coordinación con el respectivo autorizador (Jefe inmediato).
f. Los solicitantes y autorizadores son responsables de tramitar la baja de los Usuarios correspondientes a Terceros una vez que finalicen su contrato de servicio.

6.3. Uso de internet

a. El uso del Servicio de Internet es otorgado a los Colaboradores para fines laborales o para la ejecución de un servicio prestado, por lo que es controlado para optimizar su uso.
b. La autorización del servicio y el nivel de acceso en ALICORP debe ser otorgado por su respectivo autorizador.
c. Los autorizadores de ALICORP pueden revisar periódicamente los reportes de navegación (consumo por horas y páginas accedidas) del personal a su cargo, para verificar y validar que tengan los accesos correspondientes y que se use adecuadamente. Este reporte puede ser solicitado a Mesa de Ayuda.
d. Se debe hacer uso responsable del servicio de internet, con el fin de no poner en riesgo la seguridad de la información de ALICORP. Está permitido sólo para casos que estén dentro del ámbito laboral o que su función así lo requiera, lo siguiente:

   - Servicios de video, televisión y radio en línea
   - Descarga de música o video
   - Mensajería instantánea gratuita (MSN, Google Talk, etc.)
   - Skype
   - Almacenamiento en la nube (Dropbox, Google Drive, o similares)
   - Correo electrónico gratuito (Hotmail, Gmail, Yahoo, etc.)
   - Redes sociales y medios de comunicación digital

   Tener en cuenta que para éstos casos se deberá tener la aprobación previa del autorizador por jerarquía, con el sustento respectivo. No aplica para juegos en línea.

e. Para el uso de redes sociales y medios de comunicación digital, se deberán tener en cuenta las siguientes consideraciones:

   - No revelar información confidencial de ALICORP.
   - Prevenir y resguardar la imagen y reputación de ALICORP y sus marcas.
   - Solo los voceros oficiales de la compañía pueden hablar en nombre de ALICORP y sus marcas.
   - No utilizar la cuenta de correo de ALICORP para suscripciones a redes sociales y medios de comunicación digital, a menos que sean servicios relacionados a sus funciones laborales.
   - No se debe crear ni abrir perfiles en redes sociales y medios de comunicación digital en nombre de ALICORP ni de sus marcas.
   - Se recomienda no publicar fotografías o videos en los que sea visible el espacio de trabajo, las instalaciones, productos actuales o en desarrollo, logotipos de ALICORP o sus marcas, para evitar revelar información importante o confidencial.
   - Reportar el uso indebido de las redes sociales y los medios de comunicación digital, a la Vicepresidencia de Recursos Humanos Corporativos, a través de la casilla de correo: comunicacionesonline@alicorp.com.pe.

f. Se considera una falta, el ingreso a páginas Web con contenido para adultos y/o sexo explícito.
g. En caso se requiera alguna aplicación como apoyo al negocio, esta deberá ser solicitada, previa aprobación del autorizador correspondiente, a la Mesa de Ayuda siguiendo los procedimientos establecidos, evitando de esta manera la descarga de software desde Internet.

6.4. Uso de intranet (Ejemplo: Conecta)

a. El acceso a la intranet de ALICORP, será restringido sólo para los colaboradores autorizados.
b. La información mostrada en la intranet de ALICORP es de uso interno.
c. La divulgación, extracción y transferencia de la información publicada en cada intranet solo se puede realizar dentro del ámbito de ALICORP y para fines relacionado al negocio.
d. Es responsabilidad de ALICORP mantener la información actualizada en su respectiva Intranet.
e. Es responsabilidad de los colaboradores revisar periódicamente su respectiva intranet, y tomar conocimiento de la información y normatividad publicada en dicho medio.

6.5. Uso del correo electrónico corporativo

a. El uso del correo electrónico corporativo es otorgado a los Colaboradores para fines laborales. En consecuencia, todos los mensajes recibidos y enviados por correo electrónico al dominio "alicorp.com.pe" y de sus subsidiarias a nivel regional, constituyen registros de ALICORP.
b. En caso se tenga que otorgar correo electrónico corporativo a un Tercero, el usuario de correo deberá tener una nomenclatura que no lo vincule a ALICORP.
c. La aprobación para el uso del correo electrónico corporativo, debe ser otorgada por los autorizadores de ALICORP.
d. Solo se deben abrir archivos adjuntos de remitentes conocidos.
e. No deben enviarse o re-enviarse correos que contengan cadenas (SPAM), actividades ilegales, políticas o que afecten la moral.
f. El envío masivo de correos está restringido, excepto para aquellos requerimientos de Colaboradores aprobados por el autorizador por jerarquía de ALICORP.
g. Se considera una falta, disimular o falsificar la información del encabezado de un mensaje de correo electrónico corporativo, así como suplantar la identidad del colaborador que lo envía.
h. De recibir un mensaje de otra área por error, no debe revelar, copiar, distribuir o utilizar su contenido. Inmediatamente debe notificar al emisor el hecho y proceder a eliminar el mensaje de su buzón de correo electrónico corporativo.
i. La información confidencial de ALICORP solo podrá ser remitida por correo electrónico corporativo, previa aprobación del autorizador correspondiente y aplicando los criterios de seguridad recomendados para dicha clasificación.
j. De utilizarse el correo electrónico de ALICORP, de manera ocasional para el envío de información personal del colaborador, éste acepta y reconoce que se libera de su privacidad y reserva de las comunicaciones, autorizando la ejecución de los procedimientos de auditoría y monitoreo que ALICORP podría realizar en sus activos de información y equipos.
k. La configuración del correo electrónico corporativo solo está autorizada en dispositivos móviles corporativos. De requerirse su uso en dispositivos móviles personales tendrán que ser aprobados por el autorizador por jerarquía de ALICORP. Tener en cuenta que para estos casos se deberá bloquear el dispositivo utilizando una contraseña.
l. Los Colaboradores que cuenten con un usuario de correo electrónico corporativo son responsables de todas las actividades que se realizan con la misma, por lo que no deben compartir su contraseña bajo ninguna circunstancia.

6.6. Uso del servidor de archivos

a. Toda la información de ALICORP debe almacenarse en el Servidor de Archivos (Unidad P y carpeta virtual) a fin de garantizar su respaldo en copias de seguridad.
b. El acceso a las carpetas públicas (carpeta del área) debe ser aprobado por los autorizadores de ALICORP.
c. Solo se almacenará en el servidor de archivos información relacionada al negocio, quedando excluidos los archivos de música, video y fotos, excepto para aquellos casos aprobados por el autorizador por jerarquía de ALICORP.
d. El tamaño de las carpetas asignadas a los Colaboradores y las carpetas públicas debe ser limitado a través de una cuota determinada a fin de garantizar la disponibilidad del servicio. Los niveles asociados a las cuotas son asignadas por el autorizador respectivo de ALICORP.
e. La revisión de los reportes de uso de las carpetas públicas y los accesos a las mismas puede ser realizada periódicamente por los autorizadores para evitar el mal uso del servicio.

6.7. Uso de equipos de cómputo

a. El colaborador es responsable del(os) equipo(s) de cómputo que la empresa le asigne, por lo tanto debe

tomar las medidas necesarias para asegurar su protección al inicio, durante y al final del día de trabajo, no dejándolos expuestos en ambientes donde transite personal externo (terceros y visitantes) y cuidarlos de pérdidas por robo u olvido involuntario.

b. El uso del equipo de cómputo asignado a los Colaboradores es otorgado para fines laborales.
c. Toda modificación al hardware y software o cambio de ubicación del equipo asignado debe ser solicitada a la Mesa de Ayuda.
d. Los Colaboradores deben habilitar el protector de pantalla de su Equipo de Cómputo asignado al ausentarse o retirarse de su lugar de trabajo.
e. Los Colaboradores que requieren compartir información a través de una carpeta en la red, deben restringir su acceso solo para los Usuarios requeridos.
f. Se considera una falta, el uso de Equipos de Cómputo personales dentro de la red corporativa; excepto para aquellos casos aprobados por el autorizador por jerarquía de ALICORP.
g. El acceso y salida de información digital de ALICORP a través de dispositivos portátiles de almacenamiento, como discos duros externos, memorias USB, soportes magnéticos (cintas, CD, DVD) y demás dispositivos de almacenamiento externo, sólo puede realizarse previa aprobación del autorizador correspondiente de cada empresa del GR y con el sustento respectivo.
h. El uso de módems USB para acceder a internet, debe contar con la aprobación del autorizador correspondiente de ALICORP y con el sustento respectivo.
i. Todos los equipos de cómputo de los colaboradores están protegidos con un software antimalware previamente instalado.
j. Los colaboradores que estén autorizados para el uso de dispositivos de almacenamiento externo, deberán ejecutar el software antimalware al conectarlos al equipo de cómputo asignado.
k. De comprobarse un incidente de malware en el equipo de cómputo asignado al Colaborador, este será desconectado de la red corporativa para salvaguardarla, este hecho debe ser comunicado a la Mesa de Ayuda para gestionar la solución correspondiente. Para el caso de los equipos que sean propios de Terceros se tomarán las mismas acciones de mitigación, reportándose el hecho al líder de ALICORP a cargo del proyecto.

6.8. Uso de dispositivos móviles

a. Solo se podrán conectar a la red corporativa, los dispositivos móviles corporativos y personales previa aprobación del autorizador correspondiente de ALICORP.
b. Los dispositivos móviles corporativos, deben contar con un antimalware instalado y deberán estar protegidos por mecanismo de bloqueo por contraseña.
c. El uso de la funcionalidad de “bluetooth” para compartir archivos entre equipos móviles corporativos, deberá ser activada sólo cuando se requiera, y no permanentemente.

6.9. Acceso remoto (VPN o Citrix)

a. Todo Usuario para acceso remoto, requerido por los Colaboradores, debe ser aprobado y otorgado por el autorizador correspondiente de ALICORP, y configurado considerando: fecha de caducidad y servidor al que accederá.
b. Los Colaboradores que cuenten con un Usuario de acceso remoto son responsables de su uso adecuado, así como de guardar reserva de su contraseña de acceso.

7. MONITOREO:

a. ALICORP puede monitorear sus activos de información para prevenir o responder oportunamente a cualquier acción que atente contra la integridad, disponibilidad, seguridad, o desempeño correcto de los mismos mediante la negación, restricción de acceso a usuarios o sistemas, aislamiento o desconexión de equipos o servicios.
b. ALICORP puede conducir auditorías especiales sobre la información electrónica y los activos de información que son de su de propiedad.
c. Los usuarios reconocen, autorizan y se comprometen a colaborar con los procesos de auditoría e investigación, los cuales se ejecutarán cuando por alguna causa razonable se sospecha que los activos de información u equipos se han utilizado indebidamente, se han violado las políticas corporativas, se ha vulnerado la seguridad o se han realizado actividades no autorizadas, estando ALICORP autorizada por el usuario para acceder a cualquier cuenta, datos, archivos, o servicio de información asignado a los usuarios relacionados, para revisar y analizar la situación presentada.
d. Los usuarios reconocen que ALICORP tiene la autoridad para acceder archivos individuales o datos cada vez que deban realizar un mantenimiento o reparación o chequeo de los equipos de cómputo que son de su propiedad.

e. ALICORP puede restringir o prohibir el uso de sus activos de información en cualquier caso en el que exista alguna violación de estas políticas o de alguna ley.

8. DISPOSICIONES FINALES:

- El incumplimiento por parte de los colaboradores, de cualquiera de las disposiciones impartidas en la presente Política, debe ser comunicado al Jefe inmediato para que éste en coordinación con el Área de Recursos Humanos evalúe las sanciones que se puedan aplicar según el Reglamento Interno de Trabajo. Asimismo, para el caso de terceros que brindan un servicio contratado, se deberá aplicar las penalidades respectivas en coordinación con el área correspondiente.

Activo de Información	Información o recurso en formato físico o digital, relacionado con los procesos de la compañía y que tiene un valor para la misma, la cual debe ser protegida de cualquier vulnerabilidad y/o amenaza.
Autorizador (Propietario de la Información)	Persona que tiene la potestad de definir y autorizar los niveles de acceso de los Colaboradores o Terceros a los sistemas de información y servicios informáticos. Es responsable de clasificar el activo de información y de definir su nivel de riesgo aceptable y determinar quienes acceden a la información de acuerdo a sus funciones. El autorizador puede ser: • Por jerarquía: Vicepresidencia o Dirección inmediata al Colaborador o Tercero. • Por proceso: Jefatura o Gerencia responsable de un proceso de ALICORP.
Bluetooth	Protocolo de comunicaciones para redes inalámbricas que posibilita la transmisión de voz y datos entre diferentes dispositivos que se encuentran cerca
Confidencialidad	Propiedad de la información que garantiza que no esté disponible o divulgada a individuos, entidades, o a procesos no autorizados.
Disponibilidad	Propiedad de estar accesible bajo demanda de una autoridad autorizada.
Dispositivos Informáticos	Accesorio que se conecta de manera interna o externa a la PC o Laptop. Ejemplos: memoria USB, MODEM USB, CD, DVD.
Dispositivos Móviles	Aparatos de tamaño pequeño, con capacidad para procesar información, cuentan con conexión permanente o intermitente a una red y con memoria limitada. Entre estos podemos mencionar a: BlackBerrys, Smartphones y Tablets.
Equipos de cómputo	Se refiere a las Desktops, AllInOne y Laptops que son utilizadas por los Colaboradores y Terceros de ALICORP.
Hardware	Componentes físicos que forman parte de un equipo de cómputo.
Incidente de Seguridad de la Infomación (ISI)	Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información. Ejemplos: Infección de virus o malware, robo de información, Phishing, incumplimiento de políticas, etc.
Integridad	Propiedad de la información que permite salvaguardar la exactitud y completitud de los activos.
Información confidencial	Es aquella que debe ser conocida sólo por un grupo reducido de personas de la empresa. La divulgación de este tipo de información puede hacer daño a la empresa o a trabajadores de la misma. La información confidencial solamente puede ser divulgada a personas que la necesiten con fines laborales. Cuando sea necesario, el personal involucrado debe comunicar explícitamente que se trata de información confidencial. Un ejemplo de este tipo de información, son los expedientes personales o documentos con datos

	de identidad del personal de Alicorp o terceros, ya que hacen identificables a estos últimos y por lo tanto deben ser nombrados como información confidencial.
Información privilegiada	Es aquella información relacionada a negociaciones de acciones o cualquier título representativo de deuda (bonos) o propiedad (opciones) por parte de personas que tienen acceso a información no pública de la empresa.
Información de uso interno	Es aquella información que sin ser confidencial, debe mantenerse en el ámbito interno de ALICORP y no debe estar disponible externamente. Ej.: Políticas y procedimientos internos.
Malware	Es un código o software malicioso que tienen como objetivo infiltrase o dañar un equipo de cómputo o sistema de información.
Mensajería Instantánea	Sistema de intercambio de mensajes escritos en tiempo real a través de la Red.
Red	Es un sistema de comunicación entre equipos de cómputo que permite intercambiar todo tipo de información de una desktop o laptop a otra.
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Servicio de Correo Electrónico	Sistema que permite la comunicación no-interactiva de mensajes de texto, datos, imágenes o voces entre un emisario y uno o varios destinatarios por líneas de transmisión de datos.
Servicios Informáticos	Herramientas informáticas que facilitan las actividades del colaborador, tales como: correo electrónico, servidor de archivos, Internet, Mensajería Electrónica, entre otros.
Servidor de Archivos	Tipo de servidor que almacena varios tipos de archivos y los distribuye a otros colaboradores conectados a la red.
Software	Se refiere al equipamiento o soporte lógico de un equipo de cómputo, que apoya a la realización de una tarea específica. Ejemplo: Procesador de texto, aplicaciones informáticas, sistemas operativos, etc.
Spam	Correo electrónico no solicitado, de escaso o nulo interés para el receptor, usualmente de carácter comercial.
Tercero	También llamado proveedor, es toda persona (natural o jurídica) que no forma parte ALICORP y presta sus servicios.
Usuario	Identificador que es asignado a un Colaborador o Tercero que labora o presta servicios ALICORP, y que le permite el acceso a un servicio o sistema de información. Ejemplo “Jperez”.