PROGRAMA DE CIBERSEGURIDAD

CÓDIGO TI1-000-PO-001

kallpa	Fecha de vigencia:	Diciembre 2019
	Preparada por:	Gerente de TI
	Aprobada por:	Directorio
	Versión:	03
	Seguridad:	Nivel 0
PROGRAMA DE CIBERSEGURIDAD		

1. PROPÓSITO

El objetivo principal del programa de ciberseguridad es proteger los activos de información y sistemas de la Compañía. Para esto, es necesario identificar los activos críticos de la organización, gestionar de forma efectiva y oportuna todos los riesgos a los cuales se exponen los activos, concientizar y entrenar a los empleados. Con ello se busca detectar y contener todo tipo de ataque cibernético a cualquier activo mediante un sistema adecuado de gestión de la ciberseguridad basado en las mejores prácticas de ciberseguridad acorde el modelo de gestión correspondiente.

2. AMBITO Y APLICACIÓN

El presente programa aplica para los Colaboradores, contratistas, subcontratistas consultores, de la Compañía, incluyendo todo el personal afiliado a terceros que se encuentre trabajando en el manejo de información de la Compañía y utilice la infraestructura y/o los servicios tecnológicos de la Compañía

La presente política rige la interacción entre todos los activos y recursos, tanto de Tecnología de la Información como de Tecnología de Operaciones, incluyendo software (programa informático de sistema operativo, de aplicaciones de uso en nube), hardware (equipo) informático, redes y servicios en la nube, para equipos que son administrados por la Compañía (ya sean propios, alquilados o personales) o donde se encuentren los datos de la Compañía.

Este Programa de Ciberseguridad aplica a todas las compañías que forman parte de la Unidad de Negocio Perú, en adelante referidas indistintamente como Kallpa, la Empresa o la Compañía. La Unidad de Negocio Perú está integrada por Kallpa Generación S.A., Orazul Energy Perú S.A. y Kondu S.A.C.

3. REFERENCIAS NORMATIVAS

El programa de ciberseguridad está alineado con los siguientes estándares, marcos normativos y legales:

3.1. ISO 27000
Norma conceptual que se enfoca en los Sistemas de Gestión de Seguridad de la Información (SGSI).

3.2. ISO 27001
Norma certificable que establece un SGSI que incluye datos personales y cuenta con controles específicos.

3.3. Marco NIST
El Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) es una agencia del Departamento de Comercio de los Estados Unidos que proporciona un conjunto completo de normas, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad. Ofrece un enfoque de prioridades, flexible y económico para promover la protección y flexibilidad de la infraestructura crítica y otros sectores importantes para la economía y la seguridad nacional.

3.4. Norma IEC 62351
La Comisión Electrotécnica Internacional es el organismo internacional de normalización y evaluación de la conformidad para todos los campos de la electrotecnia. La norma EIC 62351 es un estándar de la industria destinado a mejorar la seguridad de los sistemas de automatización en el ámbito de los sistemas de energía.

3.5. Norma IEC 62443
Marco de ciberseguridad industrial que desarrollado por la ISA que propone un sistema de gestión de ciberseguridad de activos industriales bajo el modelo Purdue.

3.6. CIS CSC
Los Controles de Seguridad Críticos del Centro para la Seguridad de Internet es una publicación de directrices de mejores prácticas para la seguridad informática. Además, proporciona un conjunto de acciones prioritarias para proteger su organización y sus datos de los vectores conocidos de ciberataque.

3.7. Normas NERC CIP

El plan de Protección de Infraestructuras Críticas (CIP, por sus siglas en inglés) de North American Electric Reliability Corporation (NERC, por sus siglas en inglés) es un conjunto de requisitos diseñados para asegurar los activos necesarios para la operación del sistema eléctrico de Norteamérica.

3.8. Ley 29733 de protección de datos personales

Ley peruana que reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada.

4. DECLARACIÓN DE LA POLÍTICA

4.1. Descripción General

El uso de todos los recursos tecnológicos de la Compañía, los sistemas de información, activos de información, sistemas operativos y de control, comunicaciones y redes, entre otros, está sujeto al alcance de este programa y a las políticas, procedimientos y directrices específicas que se deriven del mismo.

Es responsabilidad del usuario cumplir con esta política. El área de TI es responsable de mantener esta política actualizada, de acuerdo con las necesidades del negocio y la evolución de la tecnología, asegurando la protección adecuada de los activos y operaciones de la Compañía.

4.2. Control de Acceso

4.2.1. Administración de Cuentas de Usuarios

Todos los sistemas informáticos, equipos, sistemas de control entre otros activos requieren de usuarios para poder utilizarse de forma segura.

El medio principal para verificar la identidad de un usuario es una cuenta y contraseña de usuario. Cada persona que acceda a un activo para múltiples usuarios debe utilizar una Identificación de Usuario única asignada por la Compañía y una contraseña privada. Las identificaciones de usuario no se deben compartir.

Los gerentes otorgarán derechos de acceso a los usuarios de acuerdo con su función comercial. Dicho acceso será implementado por el área de TI o el propietario de las aplicaciones cuando corresponda. Se deberá mantener registros formales de todos los derechos de acceso a cada sistema. Se sancionarán los intentos de acceso no autorizados. Se deberá informar a los proveedores de servicios sobre la política de no facilitar el acceso a los usuarios hasta que se haya otorgado una autorización específica.

Los derechos de acceso deberán ser eliminados o modificados inmediatamente después de que un usuario salga de la organización o cambie de trabajo.

4.2.2. Uso de Contraseña

Se proporcionará contraseñas temporales iniciales a todos los usuarios, las cuales deberán ser cambiadas inmediatamente según requerimiento del sistema. El área de TI será el encargado de establecer las contraseñas iniciales, las mismas que serán únicas para cada usuario. Las contraseñas temporales se otorgarán únicamente con una identificación positiva del usuario. Las contraseñas deben proporcionarse de forma segura (es decir, no en un correo electrónico de texto plano) y se mantendrán confidenciales.

Para obtener más información sobre la seguridad de las contraseñas y las directrices correspondientes, tales como longitud de la contraseña, requisitos del contenido, frecuencia de cambio, etc., sírvase consultar la Política de Contraseñas.

4.2.3. Manejo de Información

Toda la información generada y almacenada en los sistemas de información, dispositivos asignados y repositorios y/o como resultado de operaciones comerciales, se considera propiedad de la Compañía. Los usuarios podrán acceder, utilizar o compartir la información de la Compañía sólo en la medida en que ésta sea autorizada y necesaria para cumplir con las funciones laborales.

4.2.4. Confidencialidad

Para fines de la presente política, el término “Información Confidencial” se define como información relacionada con los negocios de la Compañía, generalmente desconocida para el público y con acceso limitado dentro de la Compañía, o información protegida por la ley. La “Información Confidencial” incluye

información en cualquier formato, ya sea documentos, registros o datos escritos, digitales o electrónicos.

La ISP deberá incluir información detallada sobre los privilegios de los usuarios en relación con el acceso a la información/datos, los métodos aceptados de transferencia de datos, el uso de Acuerdos de No Divulgación (NDA, por sus siglas en inglés) y el cumplimiento de la normativa.

Las preguntas relacionadas con el uso adecuado o la divulgación de Información Confidencial se deberán dirigir al supervisor inmediato y/o al Gerente de Área.

4.2.5. Cifrado

La información confidencial o sensible, según se define anteriormente, se debe proteger mediante cifrado. El área de TI proporciona un conjunto de herramientas para garantizar el cifrado en la Infraestructura de la Compañía, tales como equipos informáticos de personal clave, correos electrónicos, protocolos de transferencia de datos de gran volumen, datos de RR.HH., medios extraíbles y otros lugares en los que se almacenan o transfieren datos críticos.

4.2.6. Copia de Seguridad y Restauración

Se debe implementar un Procedimiento de Copia de Seguridad y Restauración para todas las soluciones críticas y de alta prioridad dentro de las Redes Admin e ICS. Dicho procedimiento describe el alcance, la frecuencia y el período de retención de la información.

4.3. Comunicaciones Electrónicas

Las comunicaciones electrónicas son grandes herramientas para mejorar la productividad; sin embargo, debido a la misma naturaleza de las conexiones creadas, exponen a la Compañía a riesgos cibernéticos. La Política de Comunicaciones Electrónicas define directrices específicas sobre el uso adecuado de Internet, correos electrónicos, medios de almacenamiento externo y acceso remoto, que abordan los siguientes aspectos:

4.3.1. Uso de Internet

La Compañía proporciona servicios de Internet seguro en todas sus instalaciones, para todos los Colaboradores, contratistas y visitantes. El uso de este servicio debe realizarse única y exclusivamente para cumplir las funciones laborales del usuario (Empleado, contratista, visitante) siempre en cuando se use un dispositivo de la organización o bajo las restricciones y controles impuestas para dispositivos personales. Siempre que sea posible, se utilizarán conexiones cableadas para obtener una conexión segura. Únicamente se podrá utilizar el Internet inalámbrico seguro proporcionado por la Compañía mientras se encuentre en el sitio. Se han

creado perfiles de Internet para gestionar las capacidades de navegación según los requisitos del negocio. A cada empleado se le asigna un perfil de Internet autorizado por el Gerente de área, al personal externo y contratistas se les asigna un perfil/acceso separado.

4.3.2. Correos Electrónicos

La Compañía brinda el servicio de correo electrónico a los Colaboradores que, según la naturaleza de su cargo, requieren comunicaciones electrónicas. El área de TI es el único responsable de administrar las cuentas de correo electrónico, incluyendo las listas de distribución. Todos los correos electrónicos de la Compañía pertenecen a la Compañía y pueden ser utilizados para operaciones comerciales. Es decir, cualquier correo electrónico enviado, recibido, creado o almacenado en un sistema informático

de la Compañía podrá ser monitoreado y almacenado por la Compañía como propiedad suya. Se prohíbe el uso de cualquier dirección de correo electrónico para suscribirse a cuentas o servicios no relacionados con el trabajo.

Los correos electrónicos crean una oportunidad perfecta para violar la seguridad, ya que pueden contener estafas o software malicioso para obtener credenciales, información confidencial o provocar fallas de funcionamiento del hardware. El área de TI ofrece soluciones para proteger la infraestructura de los correos electrónicos y bloquear aquellos conocidos como correos basura, no deseados y estafas. Más aún, los usuarios de correos electrónicos deben ser conscientes de los riesgos inherentes a su uso y estar capacitados para actuar de manera segura.

En caso de que un empleado no esté convencido de que el correo electrónico recibido es seguro, deberá ponerse en contacto con el área de TI.

4.3.3. Uso de Almacenamiento Externo

El uso de medios extraíbles y otros dispositivos como almacenamiento externo permite a los usuarios almacenar datos de forma separada del almacenamiento y la memoria principal o primaria de una computadora. El uso de almacenamiento externo expone los activos y sistemas de información de la Compañía a un mayor riesgo; por lo tanto, su uso debe ser controlado. Para proteger la información de la Compañía, todos los registros primarios se deben almacenar siempre en una unidad de red segura o en una plataforma en la nube, según lo determine el área de TI de la Compañía.

El Gerente de área podrá autorizar el uso de medios extraíbles a los empleados que tengan una necesidad comercial identificada para usar los mismos. Los empleados sólo podrán utilizar medios extraíbles que el área de TI haya proporcionado o aprobado explícitamente.

4.3.4. Acceso Remoto

El acceso remoto a la red de la Compañía se permite únicamente mediante el uso de una Red Privada Virtual (VPN, por sus siglas en inglés) o una herramienta específica para dicha función para el entorno industrial. En ambos casos se trata de una programación que crea una conexión segura y cifrada a través de una red menos segura, proporcionando una experiencia informática segura cuando se utilice una conexión externa. El área de TI permitirá el acceso a usuarios remotos en función de las necesidades del negocio. El usuario autorizado deberá proporcionar uno o más factores de autenticación, tales como una contraseña, un token de seguridad o datos biométricos.

4.3.5. Servicios en la Nube

A medida que la Compañía va adoptando un enfoque basado en la nube para ofrecer soluciones de negocios, resulta más relevante definir claramente los mecanismos para salvaguardar la

continuidad de los datos y las operaciones.

La contratación de proveedores que ofrecen soluciones en la nube debe seguir los mismos criterios rigurosos de evaluación y consideraciones de datos que aplican a la contratación de otros proveedores de servicios externos. Esto debe incluir, como mínimo, consideraciones explícitas sobre la propiedad de los datos, la responsabilidad para salvaguardar la seguridad y privacidad, el cumplimiento de las leyes y los Acuerdos de Nivel de Servicio (para cumplir con los requisitos de disponibilidad, desempeño y recuperación).

Las cuentas personales y/o los servicios en la nube no administrados, como Gmail o DropBox, no están respaldados y no deben utilizarse para almacenar ni transmitir información de la Compañía (confidencial o no confidencial).

4.4. Software, Hardware y Seguridad de Redes

4.4.1. Uso de Software

El software que puede ser instalado en el hardware propiedad de la Compañía es el software aprobado por el área de TI. El área de TI deberá mantener una lista de los tipos de software aprobados que estarán disponibles para los usuarios que lo soliciten.

El personal adecuado de TI se encargará de probar cualquier nuevo tipo de software para verificar su compatibilidad con el software instalado actualmente y la configuración de la red. La instalación del software sólo podrá ser realizada por personal de TI y/o personal adecuado de Operaciones cuando se encuentren realizando trabajos en los sistemas de control.

El uso o adquisición de shareware (software gratuito con tiempo limitado o restricciones) y freeware (programa informático gratuito), tales como software de código abierto o versiones de prueba, deberá ser aprobado por el área de TI. Debido a que este software, por lo general, se proporciona en un entorno de distribución abierto, se deben tomar precauciones especiales antes de instalarlo en las computadoras y redes de la Compañía.

Se prohíbe el uso de software personal o sin licencia. Queda estrictamente prohibido violar o intentar violar los términos de uso o el acuerdo de licencia de cualquier producto de software obtenido con licencia de la Compañía.

4.4.2. Antivirus y Programas para Control de Versiones

El software antivirus está instalado en todas las computadoras y servidores de la Compañía. El área de TI es el encargado de actualizar y monitorear los patrones de actualización de virus de forma directa o mediante un contrato de tercerización. A través de un procedimiento automatizado, las actualizaciones y los parches de virus se envían a las estaciones de trabajo individuales y a los servidores, según sea necesario. En el ICS se han tomado en cuenta consideraciones especiales para hardware. Los usuarios no podrán desinstalar o deshabilitar el software antivirus.

Del mismo modo, el lanzamiento de software y las actualizaciones de versiones completas son vitales, ya que proporcionan soporte para nuevas plataformas y sistemas operativos, incluyendo componentes de seguridad mejorados, por lo general, como respuesta a las vulnerabilidades identificadas.

4.4.3. Seguridad de Redes

Las redes internas y públicas de la Compañía deben estar protegidas por una arquitectura adecuada que incluya enrutadores de borde, firewalls (cortafuegos) y/o sistemas de prevención o detección de intrusiones. Solo los dispositivos autorizados podrán conectarse a las redes de la

Compañía, es decir, equipos que cumplan con las directrices de configuración de la Compañía, aprobados para su uso por el área de TI.

Los usuarios no deberán conectar a la red equipos informáticos que no pertenezcan a la Compañía o dispositivos de red que no estén autorizados o no sean propiedad de la Compañía o estén controlados por la misma.

Los dispositivos de terceros que requieran acceso a la red de la Compañía deben cumplir con todos los criterios de aceptación del sistema como si fueran dispositivos propios de la Compañía. Además, se debe controlar el acceso mediante Listas de Control de Acceso o tecnologías similares y se debe colocar en un segmento de red segregado que sólo permita autorizaciones específicas.

La autorización será solicitada por el titular del contrato y otorgada por el Gerente de TI.

Los derechos de administración de la red se limitan al personal de TI específico y se deben registrar.

4.4.4. Política de Dispositivos Móviles y de BYOD (Uso de Su Propio Dispositivo)

Los dispositivos móviles proporcionan comodidad y flexibilidad a los usuarios de la Compañía; sin embargo, son conocidos por sus vulnerabilidades inherentes. Se debe implementar una Política de Dispositivos Móviles para determinar los requisitos de seguridad de la información con el fin de proteger la información confidencial mientras se utiliza cualquier tipo de dispositivo móvil. El área de TI es responsable de proporcionar niveles de seguridad adecuados a los dispositivos móviles mediante una solución de Gestión de Dispositivos Móviles (MDM, por sus siglas en inglés) que separa la información de la Compañía, permite la eliminación remota, el cifrado, las reglas de contraseñas, el filtrado de contenidos y mucho más. Los datos que se transfieren a través de un dispositivo móvil deben estar claramente definidos y se deben aplicar las políticas correspondientes a los mismos (p. ej., sincronización de intercambios, aplicaciones móviles y otros). Adicionalmente, dicha política brinda orientación sobre las mejores prácticas de uso de equipos móviles, tales como:

- Mantener asegurada y protegida la contraseña de todos los dispositivos electrónicos
- Instalar actualizaciones de seguridad de forma regular
- Actualizar el software antivirus de forma regular
- No dejar sus dispositivos desprotegidos y expuestos
- En caso de pérdida o robo, comunicarse inmediatamente con el área de TI.

Se permite el uso de dispositivos móviles personales para acceder a la información de la Compañía; no obstante, el usuario debe cumplir con la Política de Dispositivos Móviles. En caso de pérdida o robo de un dispositivo móvil, o cambio de propiedad en el caso de dispositivos personales, el usuario debe comunicarse con el área de TI y se debe eliminar de inmediato la información, las aplicaciones y los accesos de la Compañía.

4.5. Supervisión y Prevención

4.5.1. Supervisión

Para fines de seguridad y mantenimiento de la red, las personas autorizadas dentro del área de TI o sus contratistas podrán utilizar tecnologías de vigilancia para supervisar la actividad de la red e inspeccionar los datos que se transfieren a través de esta. Las herramientas de supervisión del tráfico de red automatizadas en línea ofrecen avisos en tiempo real sobre cualquier tipo de comportamiento anormal para poder actuar ante una supuesta infracción o vulnerabilidad. Además, esta información puede correlacionarse para su análisis con el fin de desarrollar un punto de referencia de seguridad para el tráfico de Internet, el tráfico de correos electrónicos, el

tráfico de LAN (Red de Área Local), los protocolos, y la seguridad de los sistemas operativos, como mínimo. Asimismo, se puede realizar seguimiento a los registros del servidor para detectar actividades maliciosas siguiendo un cronograma de rutina, y se puede registrar otros tráficos de red, según sea necesario, para diagnosticar problemas y resolver problemas de red.

El área de TI deberá efectuar una evaluación anual de la eficacia de la política del programa de ciberseguridad, que incluirá, como mínimo, una revisión de los siguientes aspectos:

- Seguridad de la contraseña
- Dispositivos de red no autorizados
- Servidores o dispositivos webs personales no autorizados
- Conectividad remota no autorizada
- Licencias de software no autorizadas

Asimismo, toda la información y documentos a los que se acceda o se almacenen en la red de la Compañía podrán ser objeto de inspección, divulgación o eliminación.

La información obtenida como resultado de la supervisión de la red será mantenida como información confidencial y de acceso restringido. El acceso a esta información deberá ser autorizado previa justificación (investigaciones, incumplimientos, exigencias de tipo legal etc.) por parte de Gerente de TI y el Oficial de Cumplimiento. Esta información se guardará en un área de almacenamiento protegida. Los eventos e incidentes identificados a través de la supervisión de seguridad de la red se gestionarán de acuerdo con el Plan de Respuesta ante Incidentes.

4.5.2. Prueba de Vulnerabilidad y Hacking Ético

La gestión eficaz de vulnerabilidades puede reducir el riesgo para el entorno informático de la Compañía al verificar que los sistemas o dispositivos de red que utilizan niveles actuales de parches no ejecutan servicios innecesarios y no tienen contraseñas predeterminadas.

La Compañía realizará exploraciones internas de vulnerabilidades en cualquier sistema que contenga (o sistemas de acceso que contengan) datos confidenciales, al menos una vez al año. Del mismo modo, la Compañía contratará a un tercero de confianza para que realice exploraciones externas de vulnerabilidades en cualquier sistema con acceso a Internet, al menos una vez al año. Específicamente, se deberá ejecutar un hack ético para intentar explotar cualquier vulnerabilidad con el fin de determinar si existe la posibilidad de acceder al sistema sin autorización o de realizar otras actividades maliciosas en el sistema.

Las vulnerabilidades identificadas se deben ser prioritarias y se debe implementar un plan de acción dentro de los siguientes 2 meses de los Resultados de la Prueba.

4.5.3. Sensibilización y Capacitación en materia de Seguridad

Todos los usuarios estarán debidamente informados acerca de las políticas y procedimientos relevantes de Ciberseguridad de la Compañía y sobre cualquier modificación de estos. El área de Recursos Humanos es responsable de la capacitación inicial durante el proceso de orientación a los empleados. La capacitación es obligatoria antes de recibir acceso a los servicios de información o tecnología.

El área de TI es responsable de establecer el programa de concientización anual con el fin de brindar a los usuarios herramientas y conocimientos adecuados para actuar de forma segura. Dicho programa podrá incluir seminarios de capacitación interna, cursos en línea, boletines informativos por correo electrónico o intranet, carteles, etc. El cumplimiento de la capacitación anual es obligatorio.

4.6. Gestión de Incidentes de Seguridad

El término incidente de seguridad se refiere a un evento que amenaza la seguridad, integridad o disponibilidad de los recursos de información en cualquier parte de la red de la Compañía, con el riesgo potencial de perturbar las operaciones normales. La Compañía cuenta con un servicio de monitoreo continuo (CyberSOC).

Adicionalmente, cada usuario es responsable de reportar formalmente los incidentes de seguridad percibidos o las violaciones de las políticas de seguridad en forma permanente al área de TI. El área de TI debe investigar de inmediato, resolver el problema y enviar una alerta a toda la Compañía cuando sea necesario.

En materia de seguridad, la información y la puntualidad son factores clave.

El Plan de Respuesta Ante Incidentes (IRP, por sus siglas en inglés) ofrece a la Compañía una herramienta para responder sistemáticamente a los incidentes de seguridad de manera consistente, controlando el factor humano en el enfoque de respuesta. Una ISP permite a la Compañía restaurar las operaciones normales de manera más rápida y eficiente después de un incidente de seguridad. El IRP de la Compañía debe contener una lista de acciones a tomar en cada etapa del Flujo de Trabajo de Incidentes:

- Detección y Análisis
- Contención y Erradicación
- Post-Incidente

Teniendo en cuenta la forma en la que el equipo de respuesta ante incidentes comunicará, en forma interna y externa, las métricas relacionadas con la capacidad de respuesta ante incidentes y su eficacia, así como un plan de mejora continua.

5. RESPONSABILIDADES

5.1. Gerencia de TI:

- Define y mantiene el Programa de Ciberseguridad y las políticas derivadas.
- Garantiza la adecuada difusión del programa de Ciberseguridad y las políticas y procedimientos relacionados a la Compañía y a sus grupos de interés.
- Realiza una evaluación anual de riesgos cibernéticos para incorporar las lecciones aprendidas de los incidentes de seguridad, las nuevas vulnerabilidades, la regulación o los cambios en los sistemas de TI/OT de la Compañía.

5.2. Coordinador de Infraestructura y Ciberseguridad:

- Actualiza las políticas y procedimientos locales basados en la dirección corporativa.
- Garantiza la difusión adecuada de la información sobre ciberseguridad dentro de la Compañía.
- Dirige el Equipo de Respuesta ante Incidentes.

5.3. Área de Tecnología e Innovación:

- Configura Controles de Acceso de Usuarios
- Supervisa el desempeño de la red y de las aplicaciones para identificar actividades anormales.
- Realiza auditorías periódicas para garantizar el cumplimiento de las políticas.
- Realiza pruebas de vulnerabilidad periódicamente.
- Trabaja con el área de Recursos Humanos en la capacitación continua en materia de ciberseguridad para empleados y contratistas, cuando corresponda.

5.4. Gerencia de área:

- Garantiza el cumplimiento por parte de los usuarios del área (empleados y contratistas) del programa, las políticas y los procedimientos de ciberseguridad.
- Proporciona orientación sobre asuntos de confidencialidad.

- Autoriza el acceso de los usuarios del área a las aplicaciones de la Compañía, la asignación de dispositivos, el almacenamiento externo y otros recursos tecnológicos relacionados con la función de los usuarios.

5.5. Área de Recursos Humanos:

- Se encarga de que los nuevos empleados reconozcan las políticas y procedimientos de ciberseguridad.
- Brinda apoyo para llevar a cabo el programa de capacitación continua.

5.6. Usuario o Colaborador:

- Cumple con el programa de ciberseguridad, así como con sus políticas y procedimientos relacionados.

5.7. Gobernanza de Riesgo y Cumplimiento

- Brindar orientación en temas de Gobernanza Riesgo y Cumplimiento que se relacionen con esta Política
- Monitorear periódicamente la efectividad de los controles con impacto en procesos de cumplimiento

6. CONTROL Y CUMPLIMIENTO

6.1. Control y Cumplimiento

El cumplimiento de esta política es obligatorio. Todo personal deberá entender su rol y responsabilidad en relación con esta Política.

6.2. Consecuencias de Incumplimiento

Desvíos e incumplimiento del presente procedimiento puede acarrear la imposición de medidas disciplinarias, que, de aplicarse, servirán como elemento correctivo y formador de nuestra cultura organizacional.

Las medidas disciplinarias deben ser justas, razonables y proporcionales a la falta cometida, respetando el marco legal correspondiente y las normas internas de la empresa.

6.3. Excepciones

Cualquier excepción a esta política deberá tratarse de manera particular y deberá estar debidamente sustentada por el solicitante y aprobada por el CEO y el Oficial de Cumplimiento.

7. DEFINICIONES

TÉRMINO	DEFINICIÓN
Unidad de Negocio Perú	Son las compañías operativas del grupo ubicadas en el Perú. A la fecha forman parte de la Unidad de negoció Perú, Kallpa Generación S.A., Orazul Energy Perú S.A. y Kondu S.A.C.
Colaborador	Se refiere a directores, gerentes, funcionarios o empleados permanentes o temporales y practicantes o pasantes que forman parte de la Compañía.
CIS CSC (Controles de Seguridad Críticos del Centro para la Seguridad de Internet)	Los Controles de Seguridad Críticos del Centro para la Seguridad de Internet es una publicación de directrices de mejores prácticas para la seguridad informática. Además, proporciona un conjunto de acciones prioritarias para proteger su organización y sus datos de los vectores conocidos de ciberataque
Normas CIP (Protección de Infraestructuras Críticas)	El plan de Protección de Infraestructuras Críticas (CIP, por sus siglas en inglés) de North American Electric Reliability Corporation (NERC, por sus siglas en inglés) es un conjunto de requisitos diseñados para asegurar los activos necesarios para la operación del sistema eléctrico de Norteamérica

TÉRMINO	DEFINICIÓN
Infraestructura de TI (Tecnología de la Información)	Sistema de hardware, software, instalaciones y componentes de servicio que permiten la entrega de sistemas de negocios y procesos habilitados para TI.
Activos de Información	Conjunto de conocimientos que se organiza y gestiona como una sola entidad. Incluye archivos, imágenes, documentos escaneados, correos electrónicos, datos de seguimiento, normas, políticas, registros de auditoría, etc.
ICS (Sistemas de Control Industrial)	Hardware y software con conectividad de red para soportar infraestructuras críticas. Las tecnologías de ICS incluyen, pero no se limitan a, Supervisión, Control y Adquisición de Datos (SCADA, por sus siglas en inglés) y Sistemas de Control Distribuido (DCS, por sus siglas en inglés), Sistemas de Automatización y Control Industrial (IACS, por sus siglas en inglés), Controladores Lógico Programables (PLC, por sus siglas en inglés), Controladores de Automatización Programables (PAC, por sus siglas en inglés), Unidades Terminales Remotas (UTR), servidores de control, Dispositivos Electrónicos Inteligentes (IED, por sus siglas en inglés) y sensores.
Norma ISO 27000	La Organización Internacional de Normalización es una federación mundial de organismos de normalización. La norma ISO 27000 se enfoca en los Sistemas de Gestión de Seguridad de la Información.
Marco NIST (*Instituto Nacional de Estándares y Tecnología*)	El Instituto Nacional de Estándares y Tecnología es una agencia del Departamento de Comercio de los Estados Unidos que proporciona un conjunto completo de normas, directrices y mejores prácticas para gestionar el riesgo de ciberseguridad. Además, ofrece un enfoque de prioridades, flexible y económico para promover la protección y flexibilidad de la infraestructura crítica y otros sectores importantes para la economía y la seguridad nacional.
Norma IEC 62351	La Comisión Electrotécnica Internacional es el organismo internacional de normalización y evaluación de la conformidad para todos los campos de la electrotecnia. La norma EIC 62351 es un estándar de la industria destinado a mejorar la seguridad de los sistemas de automatización en el ámbito de los sistemas de energía.