

San Juan de Miraflores, 15 de enero de 2019.

**MEMORANDO N° 00014-2019-DS**

**Para** : Gerente General

**De** : Secretario General

**Asunto** : **Transcripción de Acuerdo de Directorio OD 3.**

**Referencia** : Sesión de Directorio Presencial N° 034-2018 de fecha 26 y 28 de diciembre de 2018.

Que el Directorio de la Empresa, en Sesión Presencial 034-2018 de fecha 26 y 28 de diciembre de 2018, llevada a cabo bajo la Presidencia del Ing. Luis Alberto Haro Zavaleta y con la participación de los miembros que figuran en la relación pertinente, han adoptado el siguiente acuerdo que corre en el acta respectiva, registrado con el numeral TRES, cuyo texto literal se adjunta al presente.

Atentamente,

## C E R T I F I C A C I Ó N

**EL ABOGADO QUE SUSCRIBE EN SU CALIDAD DE SECRETARIO GENERAL DE LA EMPRESA ELECTROPERU S.A., CERTIFICA QUE EN SESIÓN DE DIRECTORIO PRESENCIAL N° 034-2018 CELEBRADA EL DÍA 26 Y 28 DE DICIEMBRE DE 2018, EN FORMA UNÁNIME, SE HA ADOPTADO EL SIGUIENTE ACUERDO:**

### **O.D. 3 APROBACIÓN DE LA “POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN” DE ELECTROPERU S.A.**

El Directorio;

Considerando:

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición”, en todas las entidades integrantes del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial N° 166-2017-PCM se modificó el artículo 5° de la Resolución Ministerial N° 004-2016-PCM, a fin de efectuar determinadas precisiones en torno a la composición del Comité de Gestión de Seguridad de la Información y establecer las funciones de dicho Comité;

Que, mediante Resolución de Gerencia General N° 004-2018-G, se designó al Oficial de Seguridad de la Información;

Que, mediante Resolución de Gerencia General N°0067-2018-G, se conformó el Comité de Gestión de Seguridad de la Información;

Que, el Comité de Gestión de Seguridad de la Información, dentro de sus funciones, con fecha 17 de octubre de 2018, aprueba la propuesta de “Política de Seguridad de la Información” de ELECTROPERU S.A.;

Que, el Comité Especial de Auditoría y Riesgos en su Sesión N° 02-2018, de fecha 14 de diciembre de 2018, dispuso aprobar el texto del proyecto de la “Política de Seguridad de la Información” de ELECTROPERU S.A.;

Que, mediante el Informe Técnico N° 018-2018-AI, de fecha 17 de diciembre de 2018, el Subgerente de Informática sustenta la necesidad de aprobar la “Política de Seguridad de la Información” de ELECTROPERU S.A.

Con la conformidad del Gerente de Administración y Finanzas contenida en el Memorando N° 00433-2018-A, de fecha 18 de diciembre del 2018, la opinión favorable del Asesor Legal, contenida en el Memorando N° 00576-2018-GL y la conformidad del Gerente General, expresada en el Memorando N° 00521-2018-G, estos dos últimos de fecha 21 de diciembre del 2018; el Directorio, luego de deliberar y por unanimidad;

**ACORDÓ:**

1° Aprobar la “Política de Seguridad de la Información” de ELECTROPERU S.A; la cual como Anexo 1, forma parte integrante del presente acuerdo.

2° Encargar al Gerente General el cumplimiento del presente acuerdo y su difusión correspondiente.

ES TODO CUANTO CERTIFICO Y COMUNICO PARA LOS FINES PERTINENTES.

Lima, 2018 diciembre 26.

**ABOG. RONALD E. VALENCIA MANRIQUE**  
Secretario General

## ANEXO 1 A LA ORDEN DEL DÍA 3

### POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

#### I. OBJETIVO

Asegurar la confidencialidad, integridad y disponibilidad de la información de ELECTROPERU S.A.

#### II. ALCANCE

Todas las personas que mantienen un vínculo laboral de forma temporal o permanente y bajo todas las modalidades de contrato; así como las entidades externas y proveedores que tienen acceso a la información de la empresa.

ELECTROPERU S.A. considera la Política de Seguridad de la Información, como parte fundamental para alcanzar los objetivos de su Plan Estratégico Institucional, por lo que prioriza su difusión, comprensión y cumplimiento en todos los niveles de la organización reconociendo la necesidad de establecer un marco general con el cual se asegure que la información y sus activos sean tratados y protegidos de una manera apropiada. El anexo I muestra el 'glosario de términos' respectivo.

#### III. BASE LEGAL

- NTP-ISO/IEC 27001:2014. Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requisitos 2ª Edición
- Plan Estratégico Institucional
- Política Nacional de Gobierno Electrónico
- Ley N° 27806 - Transparencia y Acceso a la Información Pública, sus modificatorias y reglamento.
- Manual Corporativo: "Manual para la documentación de procesos y procedimientos"
- Lineamiento Corporativo: "Lineamiento de Gestión Integral de Riesgos para las empresas bajo el ámbito de FONAFE"
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital

#### IV. COMPROMISO

- Implementar, operar, monitorear, mantener y mejorar un Sistema de Gestión de Seguridad de la Información - SGSI, que permita asegurar la confidencialidad, integridad y disponibilidad de la información.
- Proveer los recursos necesarios para el cumplimiento de la Política de la Seguridad de la Información.

- Promover la concientización y capacitación al personal para que contribuyan en el cumplimiento de lo establecido en la Política de la Seguridad de la Información.
- Satisfacer requisitos aplicables relacionados a la seguridad de la información.

## ANEXO I

### GLOSARIO DE TÉRMINOS

- 1. Activo:**  
Bien vinculado a información que tiene valor para la empresa.
- 2. Confidencialidad:**  
Principio que establece que la información debe ser accesible sólo a aquellos usuarios que se encuentren debidamente autorizados.
- 3. Disponibilidad:**  
Principio que establece que la información debe estar disponible en forma organizada para los usuarios autorizados cada vez que sea requerida.
- 4. Información:**  
Considera toda la información creada, procesada, transmitida, almacenada y utilizada, que se encuentre bajo cualquier forma ya sea registro electrónico, óptico, magnético, escrita en papel o cualquier otra presentación.
- 5. Integridad:**  
Principio que establece que la información no sea alterada ni modificada, es decir, debe permanecer completa, exacta y válida.
- 6. Seguridad de la información:**  
Consiste en la preservación de la confidencialidad, integridad y disponibilidad de la información.
- 7. Sistema de Gestión de Seguridad de la Información - SGSI:**  
Sistema integral de gestión que busca establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.