# INFORME DE AUDITORÍA INTERNA DEL SGSI

1. **DATOS DE LA AUDITORÍA INTERNA**
   1. N° de auditoría: 01
   2. Norma de referencia: ISO/IEC 27001:2013
   3. Fecha de auditoría: Del 09/03/2023 al 13/03/2023
   4. Lugar de auditoría: ENSA – Remota

# OBJETIVO DE LA AUDITORIA INTERNA

Verificar la implementación, cumplimiento y eficacia del Sistema de Gestión de Seguridad de la Información de ENSA, conforme a la norma ISO/IEC 27001:2013, los requisitos legales aplicables y el logro de los objetivos propuestos, para identificar oportunidades que permitan mejorar el sistema.

# ALCANCE DE LA AUDITORIA INTERNA

ENSA, de conformidad con la ISO/IEC 27001:2013, establece que el alcance del Sistema de Gestión de Seguridad de la Información comprende los procesos/servicios:

Comercialización de Energía Eléctrica.

Operación y Mantenimiento en: Generación, Transmisión y Distribución de Energía Eléctrica.

Generación: UU.EE. Sucursales (CH de Buenos Aires). Transmisión: Zona de Concesión.

Comercialización y Distribución: Sede Corporativa Lima – Distriluz UU.EE. Chiclayo UU.EE. Sucursales

Desarrollo y Gestión de Proyectos.

De acuerdo con la Declaración de Aplicabilidad vigente.

# EQUIPO AUDITOR

* 1. Auditor Líder: José Luis Sandoval Gibaja

# FORTALEZAS Y DEBILIDADES

Entre las fortalezas más importantes del presente SGSI se encuentran:

* El compromiso demostrado de todo el personal involucrado, aún en momentos de desastres.
* El diseño del sistema de gestión engranado con el Sistema de Gestión Integrado a nivel Corporativo.
* El buen manejo que tiene ENSA respecto a sus proveedores, que pueden responder a varios controles del presente SGSI.
* La mejora continua en el ADN de sus colaboradores y la sinergia entre IT y OT.

Respecto a sus debilidades, es importante revisar y analizar con mayor profundidad en las operaciones, el ciclo de: inventario de activos, análisis de riesgos y tratamiento de riesgos.

# SOBRE LOS HALLAZGOS

Los hallazgos, como resultado de la auditoria se clasifican en:

|  |  |
| --- | --- |
| **Hallazgo** | **Significado** |
| No conformidad – NC | Incumplimiento de un requisito. |
| Observación – OB | Riesgo de incumplimiento de un requisito especificado. |
| Oportunidad de Mejora – OM | Es la sugerencia para establecer un lineamiento de mejora continua, para el SGSI. |

# RESULTADOS DE LA AUDITORÍA INTERNA

No conformidades: \_**02**\_ Observaciones: \_**05**\_ Oportunidades de mejora: \_**21**\_

Detalle de los hallazgos:

En relación con los **requisitos de la norma**, los hallazgos son los siguientes:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro.** | **Descripción del hallazgo** | **Cláusula** | **Tipo de**  **hallazgo** | **Área responsable** |
| 1 | Si bien es se verificó que el alcance del SGSI se encuentra definido como un punto en el MAPRO01.02-1 Manual de Procesos del Sistema Integrado de Gestión, se sugiere independizar dicho alcance en un documento aparte, en donde se especifique todos los requisitos establecidos como por ejemplo, la referencia al Contexto, a las Partes Interesadas y las interfaces y dependencias  entre actividades realizadas por la organización y las que son realizadas por otras organizaciones. | 4.3 | OM | SIG  CORPORATIVO  Reunión corporativa |
| 2 | Si bien se verificó indirectamente que la Alta Dirección ha comunicado la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la informaciónd, a través de las convocatorias a reuniones del Gte Corporativo de Desarrollo y Gestion de Control y algunos mails de SIG Corporativo SIG donde se informa sobre algunos temas relevantes del SGSI; se sugiere el envío de este tema en particular de manera más  explícita, como por ejemplo del Gerente General de ENSA a todos los colaboradores. | 5.1 d) | OM | SIG  Envío del correo del Gerente general - Gerente regional |
| 3 | Se recomienda continuar con el proceso de gestión de riesgos del SGSI, en particular, se encuentra en proceso la efectividad de las acciones que traten los riesgos y oportunidades del SGSI.  Además, se recomienda continuar con el proceso de Gestión de Riesgos de Seguridad de la Información  sobretodo en lo que respecta a la Aprobación de Tratamiento de Riesgos y Aceptación del riesgo | 6.1.1 e) 2)  6.1.3 f) | OM | Procesos dentro del alcance  Firma de aceptación de planes de tratamientos  Kunak |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro.** | **Descripción del hallazgo** | **Cláusula** | **Tipo de**  **hallazgo** | **Área responsable** |
|  | residual por parte del Propietario de Riesgos. |  |  |  |
| 4 | Se sugiere revisar la RESOLUCIÓN DE GERENCIA GENERAL N° GG-070-2020 puesto que en cargo del Oficial de Seguridad de la Información se señala para ENSA al Jefe de Calidad y Fiscalización, lo que podría estar en discrepancia con la GUÍA PARA EL PERFIL Y RESPONSABILIDADES DEL OFICIAL DE SEGURIDAD Y CONFIANZA DIGITAL, que en el punto IV. PERFIL DEL OFICIAL DE SEGURIDAD Y  CONFIANZA DIGITAL se puede evidenciar que las recomendaciones apuntan al puesto del Jefe de TIC. | 7.2 | OM | CORPORATIVO |
| 5 | Se sugiere como estrategia de concientización, el uso de mensajes pequeños y frecuentes para calar en la cabeza de los colaboradores. Incluir los 3 items que como mínimo obliga la norma en esta estrategia:   1. la política de seguridad de información; 2. su contribución a la efectividad del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información; y 3. las implicancias de no tener conformidad con los requisitos del sistema de gestión de seguridad de la información. | 7.3 | OM | SIG/TIC |
| 6 | En el Proceso de Comercialización y Distribución de Energía Eléctrica: Se encontraron en las oficinas de Atención al Cliente, zonas donde se guardan los expedientes del cliente sin llaves que pudieran estar expuestos a riesgos por pérdida o robo ya que son zonas de acceso al público en general. De igual manera el Libro de Observaciones, sería recomendable una cadena. Y el uso de puertas  vaiven. | 8  A.8.1.1 | OB | Gestión comercial  Kunak  Canalizar a través de Seguridad Patrimonial y Logística |
| 7 | En el Proceso de Desarrollo y Gestión de Proyectos: Se sugiere profundizar el análisis del riesgo de la documentación en papel de los expedientes de los proyectos en las oficinas y en las zonas de almacenamiento, puesto que pudieran estar expuestos a pérdidas y el impacto legal por sanciones podría ser fuerte. Así mismo, el uso de  puertas vaiven sería recomendable para minimizar la probabilidad de estas pérdidas. | 8  A.8.1.1 | OM | Desarrollo y gestión de proyectos  Kunak  Canalizar a través de Seguridad Patrimonial y Logística |
| 8 | Si bien, se verificó que el monitoreo, medición, análisis y evaluación del SGSI se realiza a través del Plan Operativo y que el área de Planeamiento hace el seguimiento, se recomienda considerar en este seguimiento los **procesos** y **controles** para seguridad. | 9.1 a) | OM | CORPORATIVO |
| 9 | Si bien, se está esperando terminar con el proceso de Auditoría Interna para considerarlo dentro de la próxima Revisión por la Dirección del Sistema de Gestión Integrado, se sugiere tener una plantilla de  la ppt que se mostrará para incorporar todos los elementos mandatorios que como mínimo se deben | 9.3 | OM | SIG  KUNAK  Actas de revisión y ppt plantilla |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro.** | **Descripción del hallazgo** | **Cláusula** | **Tipo de**  **hallazgo** | **Área responsable** |
|  | revisar para cumplir con la ISO/IEC 27001. |  |  |  |
| 10 | Si bien, se tiene considerado dentro del procedimiento P01.02.01.06-1 Acciones Correctivas y Oprtunidades de Mejora, los lineamientos para la toma de acción ante no conformidades, se recomienda tener en cuenta los otros elementos de entrada para la toma de acciones correctivas, no sólo las Auditorías Internas y Externas. Como por ejemplo: eventos e incidentes de seguridad de la  información, debilidades de seg. de la inf., etc. | 10.1 | OM | SIG  Indicadores trimestralmente de TIC; poner en copia al OSD para que los indicadores se cumplan |
|  |  |  |  |  |

En relación con el anexo A de la norma, los hallazgos son los siguientes:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro.** | **Descripción del hallazgo** | **Domino / Obj. de Control / Control** | **Tipo de**  **hallazgo** | **Área responsable** |
| 1 | Se sugiere continuar con el proyecto de Acuerdos de Confidencialidad y Carta de Compromiso. | A.7.3.1 | OM | Gestión de personas |
| 2 | La asignación y uso de derechos de acceso privilegiado, como el rol de Administradores, debe ser restringida y controlada, como por ejemplo, a través del F22.01-03 aprobado formalmente. | A.9.2.3 | OB | TIC  Formalizar los roles |
| 3 | Se sugiere incluir al sistema SCADA en la revisión  de derechos de acceso formal. | A.9.2.5 | OM | TIC/OPERACIONES |
| 4 | Se sugiere en general en las oficinas que requieran por ser zonas seguras, el uso de dispositivos vaiven para asegurar tener cerradas  las puertas de acceso. | A.11.1.2 | OM | SEGURIDAD PATRIMONIAL  LOGISTICA |
| 5 | Se sugiere el uso de herramientas como por ejemplo BitLocker, para la seguridad de los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización. Por ejemplo robo de notebooks y los discos duros quedan  expuestos. | A.11.2.6 | OM | TIC |
| 6 | Al estar configurado en el AD la GPO para la activación del screensaver luego de 30 minutos de inactividad, se sugiere analizar los riesgos de este tiempo del equipo desatendido. Si se mantiene la política con dicho tiempo, evaluar reforzar la concientización a los usuarios de tal manera que cuando se levanten de sus sitios, bloqueen la  sesión. | A.11.2.8 | OM | TIC |
| 7 | Se sugiere coordinar con el Corporativo de tal manera que se pueda tener acceso a la Bitácora de Cambios y se pueda evidenciar los cambios en la organización, procesos de negocio, instalaciones de procesamiento de información y | A.12.1.2 | OM | CORPORATIVO  Solicitar la bitácora |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro.** | **Descripción del hallazgo** | **Domino / Obj. de Control / Control** | **Tipo de**  **hallazgo** | **Área responsable** |
|  | sistemas. |  |  |  |
| 8 | Revisar el responsable de la revision de los logs  en SCADA y asegurar su cumplimiento. | A.12.4.1 | OM | OPERACIONES/TIC |
| 9 | En el item 4 a) Política de Transferencia de Información, dice en el punto f) que toda información enviada a través del correo institucional debe incluir una ADVERTENCIA en cuanto a su uso y autorizaciones al respecto. Ello no se viene cumpliendo en la actualidad. | A.13.2.1  A.13.2.3 | NC | CORPORATIVO  TIC |
| 10 | Para los requerimientos de nuevos sistemas o mejoras o cambios a los sistemas, no se ha incluído los requisitos de Seguridad de la Informacion. Ver el FC22-01 | A.14.1.1 | OB | CORPORATIVO  HIDRANDINA |
| 11 | Revisar los riesgos respecto al uso de datos de prueba en ambientes de desarrollo y/o pruebas con el proveedor actual, de tal manera que se pueda decidir el uso de herramientas de, por ejemplo,  ANONIMIZACIÓN. | A.14.3.1 | OM | CORPORATIVO  GRUPO DE DESARROLLO  HIDRANDINA |
| 12 | No se pudo evidenciar una Política de Seguridad de la Información para las relaciones con los proveedores, que haya sido aprobada, que se encuentre en uso y que haya sido comunicada a los proveedores. | A.15.1.1 | NC | CORPORATIVO  LOGISTICA DE CADA UNA DE LAS EMPRESAS |
| 13 | Se sugiere estandarizar la cláusula de CONFIDENCIALIDAD usada en los contratos y/o los TDRs, de tal manera que se aborde la seguridad de la información de una manera estándar, considerando todos los requisistos de seguridad de la información, según el proveedor. | A.15.1.2 | OM | LOGISTICA |
| 14 | Se sugiere incorporar un item (a manera de guía a los usuarios que reportan) de los tipos de debilidades, eventos e incidentes de seguridad de información, que incluyan no sólo lo relacionado a TI sino también, temas relacionados a las personas, a la infraestructura, temas de Operaciones, etc. que podrían ser contempladas y, además, colocar a quien se reporta según el  tema. | A.16.1.2  A.16.1.3 | OM | CORPORATIVO  ACTUALIZACIÓN DEL PROCEDIMIENTO |
| 15 | No se ha podido evidenciar la lista de Obligaciones Legales y Otros Requisitos en ENSA, relacionados a seguridad de la información. | A.18.1.1 | OB | CORPORATIVO |
| 16 | Se sugiere, en la medida de lo posible, usar el Inventario de Licencias que sirve para responder el A.18.1.2, conectarlo también con Gestión de la Capacidad para evidenciar el control de un  recurso importante como son las licencias. | A.18.1.2 | OM | TIC  ACTUALIZACIÓN DEL MANUAL DE CONTROLES |
| 17 | Se revisaron las Resoluciones Directorales N° 3849-2015-JUS/DGPDP-DRN de fecha 18 de  noviembre del 2015 y se sugiere mejorar el apartado: “Dirección para el ejercicio de los derechos de acceso, rectificación, cancelación y oposición:” puesto que hace referencia a correos | A.18.1.4 | OM | TIC – Correos generales  Gestión de la Resolución – Gestión de personas |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nro.** | **Descripción del hallazgo** | **Domino / Obj. de Control / Control** | **Tipo de**  **hallazgo** | **Área Responsable** |
|  | personales [jayalac@distriluz.com.pe](mailto:jayalac@distriluz.com.pe) y [ksilvaf@distriluz.com.pe](mailto:ksilvaf@distriluz.com.pe) que podrían variar en el tiempo al ser de colaboradores que podrían o  cambiar de roles o salir de la organización. |  |  |  |
| 18 | No se ha podido evidenciar que de manera anual ENSA realice las evaluaciones técnicas de vulnerabilidades, tal como se establece en el Manual de Controles en el item 3 a). | A.18.2.3 | OB | TIC  CORPORATIVO |
|  |  |  |  |  |

# CONCLUSIONES DE LA AUDITORIA

* Se ha evidenciado el compromiso de todo el personal con el Sistema de Gestión de la Seguridad de la Información a través de la revisión de los registros auditados.
* Se logró cumplir con el Programa de la Auditoría Interna.
* Estamos frente a un Sistema de Gestión bien diseñado en fase de mejora. El resultado de la presente auditoría evidencia esta conclusión con 21 Oportunidades de Mejora, frente a 2 No Conformidades y 5 Observaciones, hablan de que en general se están cumpliendo los requisitos de la norma y ahora lo que se espera es mejorar.
* La orientación a la mejora continua de ENSA ha sido evidenciada en cada uno de los puntos revisados.
* La sinergia entre IT y OT ha sido evidenciado.

# FIRMA DEL AUDITOR LÍDER



Nombre: José Luis Sandoval Gibaja DNI: 09576491