SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

ZONA REGISTRAL NºIX – SEDE LIMA

RESOLUCIÓN JEFATURAL N°789-2022-SUNARP/ZRIX/JEF

Lima, 11 de noviembre de 2022

VISTOS; el Memorándum Nº00025-2022-SUNARP/ZRIX/JEF/JEF-SIG-SGSI del 07 de noviembre de 2022; el Memorándum Nº01608-2022-SUNARP/ZRIX/UPPM del 08 de noviembre de 2022; el Memorándum Nº00941-2022-SUNARP/ZRIX/UAJ del 09 de noviembre de 2022; el Memorándum Nº00049-2022-SUNARP/ZRIX/JEF/JEF-SIG del 10 de noviembre de 2022, y;

CONSIDERANDO:

Que, mediante el artículo 1° de la Ley N°26366, Ley de Creación del Sistema Nacional de los Registros Públicos y de la Superintendencia de los Registros Públicos, publicada en el Diario Oficial "El Peruano" el 16 de octubre de 1994, se crea el Sistema Nacional de los Registros Públicos con la finalidad de mantener y preservar la unidad y coherencia del ejercicio de la función registral en todo el país, orientado a la especialización, simplificación, integración y modernización de la función, procedimientos y gestión de todos los registros que lo integran;

Que, mediante el artículo único de la Ley N°27309, publicado en el Diario Oficial "El Peruano" el 17 de julio de 2000, se modifica el Título V del Libro Segundo del Código Penal, incorporándose los Delitos Informáticos;

Que, mediante el artículo 1° de la Ley N°27658, Ley Marco de Modernización de la Gestión del Estado, publicada en el Diario Oficial "El Peruano" el 30 de enero del 2002, se declaró al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, por Decreto Supremo N°052-2008-PCM, publicado en el Diario Oficial "El Peruano" el 19 de julio de 2008, se aprobó el Reglamento de la Ley de Firmas y Certificados Digitales, con el objeto de regular, para los sectores público y privado, la utilización de las firmas digitales y el régimen de la Infraestructura Oficial de Firma Electrónica;

Que, mediante Decreto Supremo N°004-2013-PCM, publicado en el Diario Oficial "El Peruano" el 09 de enero de 2013, se aprobó la Política Nacional de Modernización de la Gestión Pública, siendo el principal instrumento orientador de la modernización de la gestión pública en el Perú, que establecerá la visión, los principios y lineamientos para una actuación coherente y eficaz del sector público, al servicio de los ciudadanos y el desarrollo del país;

Que, por Resolución Ministerial N°004-2016-PCM, publicado en el Diario Oficial "El Peruano" el 14 de enero de 2016, 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 y su modificatoria;

Que, por Resolución Directoral N°056-2017-INACAL/DN, publicado en el Diario Oficial "El Peruano" el 29 de diciembre de 2017, se aprobó la Norma Técnica Peruana NTP-ISO/IEC 27002:2017, Tecnología de la Información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información. 1ª Edición;

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

ZONA REGISTRAL NºIX – SEDE LIMA

RESOLUCIÓN JEFATURAL N°789-2022-SUNARP/ZRIX/JEF

Lima, 11 de noviembre de 2022

Que, mediante Resolución de la Superintendente Nacional de los Registros Públicos N°208-2008-SUNARP/SN del 17 de julio de 2008, se aprueba la Directiva N°004-2008-SUNARP/SN, denominada "Normas para la Administración, Uso y Control del Servicio de Publicidad Registral en Línea";

Que, mediante Resolución de la Gerencia General de la Superintendente Nacional de los Registros Públicos N°210-2022-SUNARP/GG del 04 de julio de 2022, se aprobó la Directiva DI-002-2022-UOM-OPPM, denominada *"Directiva que regula la emisión de los documentos normativos de la Sunarp",* que establece las disposiciones para la formulación, aprobación, emisión, revisión, actualización y derogación de los documentos normativos;

Que, de acuerdo al artículo segundo de la Resolución Jefatural N°350-2018-SUNARPZ.R.N°IX/JEF del 18 de junio de 2018, se designó como Supervisor de Seguridad de la Información de la Zona Registral N°IX-Sede Lima, al Analista de Producción de la Unidad de Tecnologías de la Información, Ingeniero Armando Ángel Marchetti Espejo; asimismo, con el artículo segundo de la Resolución Jefatural N°391-2020-SUNARP-Z.R.N°IX/JEF del 19 de noviembre de 2020, se modificó la denominación de Coordinador por la de "Oficial" a los responsables de cada uno de los sistemas de gestión a quienes a partir de esa fecha se les identificará conforme se detalla: Oficial del Sistema de Gestión de Calidad, Oficial del Sistema de Gestión de Seguridad de la Información, Oficial del Sistema de Seguridad y Salud en el Trabajo;

Que, mediante Resolución Jefatural N°271-2020-SUNARP-Z.R.N°IX/JEF del 21 de agosto de 2020, se conformó el Comité del Sistema Integrado de Gestión – SIG de la Zona Registral N°IX-Sede Lima, cuya responsabilidad principal es actuar como un ente rector de gestión, a cargo de desarrollar las tareas de planificación y seguimiento del Sistema Integrado de Gestión, absorbiendo las funciones del Comité de Gestión de Calidad;

Que, mediante Resolución Jefatural N°663-2022-SUNARP/ZRIX/JEF del 27 de setiembre de 2022, se aprobó por cambio de versión el Manual de políticas Específicas de Seguridad de la Información (versión: 02, Código: MN-001-JEF-ZRIX);

Que, mediante Resolución Jefatural N°702-2022-SUNARP/ZRIX/JEF del 11 de octubre de 2022, se aprobó por cambio de versión, el Procedimiento de Gestión de Documentos de Soporte a los Procesos (Versión: 04, Código: PR-003-UPP-ZRIX);

Que, mediante Resolución Jefatural N°768-2022-SUNARP/ZRIX/JEF del 03 de noviembre de 2022, se designó Coordinador General del Sistema Integrado de Gestión al analista de Producción de la Unidad de Tecnologías de la Información, ingeniero Armando Ángel Marchetti Espejo;

Que, mediante Memorándum Nº00025-2022-SUNARP/ZRIX/JEF/JEF-SIG-SGSI, el Oficial del Sistema de Gestión de Seguridad de la Información remite a la Unidad de Planeamiento, Presupuesto y Modernización, el proyecto del Manual de Políticas Específicas de Seguridad de la Información, versión 03, con el debido sustento técnico, para su revisión;

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

ZONA REGISTRAL NºIX – SEDE LIMA

RESOLUCIÓN JEFATURAL N°789-2022-SUNARP/ZRIX/JEF

Lima, 11 de noviembre de 2022

Que, mediante Memorándum N°00941-2022-SUNARP/ZRIX/UAJ, el Jefe de la Unidad de Asesoría Jurídica, remite al Coordinador General del Sistema Integrado de Gestión, el proyecto del Manual en mención, con la opinión legal favorable, en atención a lo requerido por Memorándum N°01608-2022-SUNARP/ZRIX/UPPM del 08 de noviembre de 2022, emitido por la Jefe de la Unidad de Planeamiento, Presupuesto y Modernización, con la opinión favorable de su Unidad respecto del contenido, estructura y sustento técnico del citado proyecto;

Que, mediante Memorándum N°00049-2022-SUNARP/ZRIX/JEF/JEF-SIG, el Coordinador General del Sistema Integrado de Gestión, informa a la Unidad de Asesoría Jurídica que, en reunión de Comité del Sistema Integrado de Gestión de fecha 08 de noviembre de 2022, a través de Acta N°019-2022, se aprobó el Manual de Políticas Específicas de Seguridad de la Información, en su tercera versión; asimismo, solicita la emisión del documento normativo correspondiente a fin de concluir con el flujo de aprobación;

Que, esta Jefatura considera pertinente aprobar, por cambio de versión, el Manual de Políticas Específicas de Seguridad de la Información (Versión: 03, Código: MN-001-JEF-ZRIX), el mismo que cuenta con la aprobación del Comité del Sistema Integrado de Gestión, según Acta N°019-2022 del 08 de noviembre de 2022;

Con las visaciones de la Coordinador General del Sistema Integrado de Gestión y Oficial de Seguridad de la Información, del Jefe de la Unidad de Tecnologías de la Información, de la Jefe de la Unidad de Planeamiento, Presupuesto y Modernización, y del Jefe de la Unidad de Asesoría Jurídica;

En uso de las atribuciones conferidas por el Consolidad del Texto Integrado del Reglamento de Organización y Funciones de la Sunarp, aprobado por Resolución de la Superintendencia Nacional de los Registros Públicas N°035-2022-SUNARP/SN, el Manual de Operaciones de los Órganos Desconcentrados de la Sunarp, aprobado por Resolución de la Superintendencia Nacional de los Registros Públicos N°155-2022-SUNARP/SN y en virtud de la Resolución de la Gerencia General de la Superintendencia Nacional de los Registros Públicos N°336-2021-SUNARP/GG del 16 de diciembre de 2021.

SE RESUELVE:

Artículo 1.- Aprobación por cambio de versión, el Manual de Políticas Específicas de Seguridad de la Información

Apruébese por cambio de versión, el Manual de Políticas Específicas de Seguridad de la Información (Versión: 03, Código: MN-001-JEF-ZRIX), el mismo que como anexo forma parte integrante de la presente Resolución.

Artículo 2.- Dejar sin efecto

Déjese sin efecto la Resolución Jefatural N°663-2022-SUNARP-ZRIX/JEF del 27 de setiembre de 2022, que aprobó por cambio de versión, el Manual de Políticas Específicas de Seguridad de la Información (Versión: 02, Código: MN-001-JEF-ZRIX),

SUPERINTENDENCIA NACIONAL DE LOS REGISTROS PÚBLICOS

ZONA REGISTRAL NºIX – SEDE LIMA

RESOLUCIÓN JEFATURAL N°789-2022-SUNARP/ZRIX/JEF

Lima, 11 de noviembre de 2022

Artículo 3.- Difusión

Disponer que, a través de la Unidad de Comunicaciones, se ejecuten las acciones respectivas destinadas a su publicación en la página web institucional con la finalidad de que todas las áreas tomen conocimiento y brinden las facilidades del caso, cuando corresponda.

Regístrese, comuníquese y publíquese en el portal institucional.

Firmado digitalmente por:
PEREZ SOTO Jose Antonio FAU 20260998898 soft
Motivo: Soy Autor del Documento
Fecha: 2022/11/11 21:04:18-0500

Firmado digitalmente
JOSÉ ANTONIO PÉREZ SOTO
Jefe Zonal (e)
Zona Registral N°IX-Sede Lima - SUNARP

sunarp Superintendencia Nacional de los Registros Públicos	Tipo de documento: **MANUAL**		Código: **MN-001-JEF-ZRIX**
	Aprobación:	**Resolución N°789-2022- SUNARP-ZRIX/JEF**	
	Versión: **V.03**	Fecha de aprobación: **11/11/2022**	Páginas: **1/42**

MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

ÍNDICE

I. OBJETIVO

Describir la aplicación de controles de Seguridad de la Información de la Norma ISO 27001 en la Zona Registral N° IX – Sede Lima, con excepción de los controles excluidos en la declaración de aplicabilidad.

II. ALCANCE

El presente manual es de obligatorio cumplimiento para las Unidades Orgánicas que desarrollan actividades en los procesos comprendidos en el alcance del Sistema de Gestión de Seguridad de la Información que forma parte del Sistema Integrado de Gestión de la Zona Registral N° IX – Sede Lima.

III. BASE LEGAL

La siguiente documentación contiene disposiciones que, al ser citadas en este texto, constituyen requisitos de este manual.

3.1. Ley N° 26366 – Ley de Creación del Sistema Nacional de los Registros Públicos y de la Superintendencia de los Registros Públicos, de fecha 16 de octubre de 1994 y su modificatoria.

3.2. Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal, de fecha 17 de julio de 2000.

3.3. Decreto Supremo N° 008-2004-JUS, que aprueba el Texto Único de Procedimientos Administrativos – TUPA de la Superintendencia Nacional de los Registros Públicos, de fecha 01 de agosto de 2004.

3.4. Decreto Supremo N° 052-2008-PCM que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales, de fecha 19 de julio de 2008 ***y sus modificatorias.***

3.5. Resolución Ministerial Nº 004-2016-PCM, Aprueban 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, ***de fecha 08 de enero de 2016*** y su modificatoria.

3.6. Resolución del Superintendente Nacional de los Registros Públicos N° 208-2008-SUNARP/SN, que aprueba la Directiva N° 004-2008-SUNARP/SN denominada “Normas para la Administración Uso y Control del Servicio de Publicidad Registral en Línea”, de fecha 17 de julio de 2008 ***y sus modificatorias.***

3.7. Resolución del Superintendente Nacional de los Registros Públicos N° 126-2012-SUNARP/SN, que aprueba el Texto Único Ordenado del Reglamento General de los Registros Públicos, de fecha 18 de mayo de 2012 y su modificatoria.

IV. TÉRMINOS Y DEFINICIONES

Los términos y definiciones usados en el Sistema de Gestión de Seguridad de la Información de la Zona Registral N° IX - Sede Lima son tomados de la Norma ISO 27001, los cuales son:

4.1. Activo: En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

4.2. Activo de información: Conocimientos o datos que tienen valor para Zona Registral N° IX – Sede Lima.

4.3. Confidencialidad: Propiedad que determina que la información no esté disponible, ni sea divulgada a personas, entidades o procesos no autorizados.

4.4. Disponibilidad: Propiedad de ser accesible y utilizable cuando lo requiera una entidad autorizada.

4.5. Estación de trabajo: Equipo de cómputo también llamado computadora personal que normalmente está conectada a la red informática y es usada por el servidor civil como herramienta de trabajo para conectarse a sistemas de información, u otros servicios, tales como correo electrónico, internet, etc.

4.6. Incidente de seguridad de la información: Uno solo o serie de eventos de seguridad de la información, no deseados o inesperados, que tiene una probabilidad significativa de comprometer operaciones de negocio y amenazar la seguridad de la información.

4.7. Información: Conjunto de datos contenidos en documentos físicos (Papel, Microfichas, Libros, etc.), medios magnéticos (Cintas, Cartridge, Discos), medios ópticos (CD's, CDR, CDRW, DVD, etc.) y medios electrónicos (USB, Disco Duro Externo, etc.).

4.8. Integridad: Propiedad de salvaguardar la exactitud y completitud de los activos.

4.9. Propietario del activo: Identifica a la persona o la entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, desarrollo, mantenimiento, uso y seguridad de los activos. Tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.

4.10. Seguridad de la información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información.

4.11. Sistema de información: Aplicaciones, servicios, activos de tecnología de información, u otros componentes de manejo de la información.

4.12. Usuario: Persona registrada y autorizada a utilizar un sistema de información determinado, bajo un nivel de acceso pre-establecido.

V. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN (ISO 27001-A.5)

5.1. DIRECCIÓN DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN [ISO 27001 A.5.1]

5.1.1. Políticas de seguridad de información [ISO 27001 A.5.1.1]

a) Las políticas de seguridad de la información deben establecer las directivas y requerimientos necesarios para implementar un razonable nivel de protección de los activos de información de la Zona Registral N° IX - Sede Lima y deben estar plasmadas en el documento “Política del Sistema Integrado de Gestión”, “Manual del Sistema Integrado de Gestión” y en el presente “Manual de Políticas Específicas de Seguridad de la Información”.

b) Las políticas de seguridad de la información deben ser aprobadas, publicadas y comunicadas según la “Matriz de comunicaciones” ***del Sistema Integrado de Gestión.***

5.1.2. Revisión de las políticas de seguridad de información [ISO 27001 A.5.1.2]

Se deben realizar revisiones y mantenimiento de las políticas de seguridad de información por lo menos una vez al año o cuando ocurran cambios significativos, por parte del Oficial del Sistema de Gestión de Seguridad de la Información - SGSI y del Coordinador General del Sistema Integrado de Gestión - SIG.

VI. ORGANIZACIÓN DE SEGURIDAD DE INFORMACIÓN (ISO 27001-A.6)

6.1. ORGANIZACIÓN INTERNA [ISO 27001 A.6.1]

6.1.1. Funciones y responsabilidades para la seguridad de la información [ISO 27001 A.6.1.1]

a) La Zona Registral N° IX - Sede Lima constituye un Comité del Sistema Integrado de Gestión (Comité del SIG), el cual asume la responsabilidad sobre el Sistema de Gestión de Seguridad de la Información de la Zona Registral N° IX - Sede Lima, según se indica en el “Manual del Sistema Integrado de Gestión”.

b) El Jefe de la Zona Registral N° IX - Sede Lima debe designar a un Oficial de SGSI, el cual es responsable de la administración del Sistema de Gestión de Seguridad de la Información de la Zona Registral N° IX - Sede Lima.

c) Las funciones y responsabilidades del personal de la Zona Registral N° IX - Sede Lima y terceros con respecto al Sistema de Gestión de Seguridad de la Información se encuentran indicados en el “Manual del Sistema Integrado de Gestión”, “Procedimiento para la Gestión de Riesgos del Sistema Integrado de Gestión”, “Instructivo de Evaluación y Tratamiento de Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información” y en los procedimientos específicos.

6.1.2. Separación de Funciones [ISO 27001 A.6.1.2]

a) Los propietarios de los activos de información deben autorizar el acceso teniendo en consideración una adecuada definición y

segregación de funciones, de acuerdo a las actividades y funciones de las unidades de organización.

b) Se debe asegurar que todos los roles y responsabilidades se encuentren definidos en “Manual del Sistema Integrado de Gestión”, “Procedimiento para la Gestión de Riesgos del Sistema Integrado de Gestión”, “Instructivo de Evaluación y Tratamiento de Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información” y en los procedimientos específicos, para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

6.1.3. Contacto con autoridades [ISO 27001 A.6.1.3]

La Zona Registral N° IX - Sede Lima cuenta con una lista de teléfonos de emergencia del Sistema de Gestión de Seguridad y Salud en el Trabajo - SGSST con las autoridades encargadas de vigilar el cumplimiento de la normativa aplicable a las cuales se debe acudir ante algún incidente ***de seguridad de la información***, dicha lista se encuentra en carteles pegados en las diversas oficinas de la entidad como parte del SGSST.

6.1.4. Contacto con grupos de interés especial [ISO 27001 A.6.1.4]

a) El Oficial SGSI de la Zona Registral N° IX - Sede Lima debe registrarse en foros que le envíen actualizaciones respecto a seguridad de información y debe mantener constante relación con las entidades externas que puedan prestar apoyo en caso de incidentes de seguridad de la información, la relación deberá mantenerse a un nivel tal que asegure el apoyo, pero sin generar obligaciones de entregar información confidencial.

b) El contacto con grupos de interés especial deberá estar en el formato “Lista de Contacto con Grupos de Interés Especial del Sistema de Gestión de Seguridad de la Información”. ***Asimismo, el Oficial del SGSI debe mantener contacto y coordinar con el Oficial de Seguridad Digital - OSD de la Sede Central.***

6.1.5. Seguridad de información en gerencia de proyectos [ISO 27001 A.6.1.5]

La seguridad de la información debe integrarse en el método de gestión de proyectos de la Zona Registral N° IX - Sede Lima para garantizar que los riesgos de seguridad de la información son identificados y tratados como parte de un proyecto, alineados a las buenas prácticas del PMI, ***según lo indicado en el formato Plan de Gestión del Proyecto.***

6.2. DISPOSITIVOS MÓVILES Y TELETRABAJO [ISO 27001 A.6.2]

6.2.1. Política de dispositivo móvil [ISO 27001 A.6.2.1]

a) La Zona Registral N° IX - Sede Lima debe establecer la presente Política de Dispositivos Móviles:

- Se debe considerar como dispositivos móviles a todos aquellos equipos informáticos que realicen el procesamiento de información, que tengan conexión a internet y con memoria

limitada, como son las Laptops, Tablet, Celulares, tokens y similares.

- Se debe contar con un adecuado registro de los dispositivos móviles.
- Todos los servidores civiles que tengan asignado un dispositivo móvil deben asegurar una adecuada protección física del dispositivo móvil para asegurar la integridad del mismo, asimismo asegurarse de que ***las laptops*** tengan las versiones actualizadas de los productos de software que tengan instalados.
- ***Todos los servidores civiles que ingresan a un dispositivo diferente al propio deben cerrar la sesión del correo y los aplicativos.***
- ***Todos los servidores civiles que ingresan a un dispositivo diferente al propio deben eliminar toda la información confidencial que hayan trabajado en el dispositivo, asimismo de la papelera al finalizar su presentación o labor.***
- Los parches o actualizaciones serán obtenidos de manera formal, provenientes del fabricante.
- Los dispositivos móviles deberán contar algún medio de autenticación (usuarios, pin, patrón de desbloqueo u otro mecanismo), que permita que solo el propietario del activo de información pueda tener acceso al dispositivo. ***Siendo el propietario del activo el responsable de activar esta autenticación*.**

6.2.2. Teletrabajo [ISO 27001 A.6.2.2]

a) La Zona Registral N° IX - Sede Lima debe establecer la presente Política de Trabajo remoto y Teletrabajo:

- El trabajo remoto y teletrabajo se ejecuta fuera del centro habitual de trabajo, en el domicilio o lugar de ubicación del servidor, a través de herramientas tecnológicas de propiedad del servidor o de la Zona Registral N° IX - Sede Lima, entregados en calidad de préstamo, acuerdo individual o convenio, accediendo a los servicios utilizados habitualmente en sus labores registrales o administrativas.
- El servicio de acceso remoto debe permitir el ingreso a la red de datos a aquellos usuarios externos e internos expresamente autorizados por los jefes de las Unidades Orgánicas correspondientes, el cual debe estar sujeto a autenticación con un nivel adecuado de protección y obedecer a necesidades justificadas.
- Los equipos de los servidores civiles (PC), los equipos de procesamiento de datos tipo servidor y de comunicaciones podrán tener habilitado el servicio de conexión de acceso remoto vía VPN.

- Los servidores civiles para acceder a estos recursos serán previamente identificados y autorizados.
- Cualquier servidor civil autorizado que requiera acceso a la red desde el exterior debe estar debidamente autenticado con doble factor de autenticación y su conexión se debe realizar mediante la VPN.
- ***El servidor civil será el responsable de dar la seguridad física de la PC o laptop en el sitio del trabajo remoto y proteger el acceso de personas no autorizadas a la información o recursos de la Entidad.***

VII. SEGURIDAD DE RECURSOS HUMANOS (ISO 27001-A.7)

7.1. ANTES DEL EMPLEO [ISO 27001 A.7.1]

7.1.1. Selección [ISO 27001 A.7.1.1]

a) La Unidad Recursos Humanos ***- URH*** debe mantener expedientes de verificación de todos los postulantes que ganaron un concurso, en concordancia con las leyes, regulaciones, ética y requerimientos. Dichos expedientes deben tomar en consideración la privacidad y la protección de los datos del candidato, incluyendo lo siguiente:

- La ***solicitud de la*** comprobación de los documentos de identificación, por ejemplo: currículo vitae, certificados académicos y profesionales.
- Comprobaciones más detalladas, por ejemplo: antecedentes penales y/o, policiales.
- Para la evaluación de los trabajadores de la Zona Registral N° IX - Sede Lima, la URH debe seguir los lineamientos establecidos en el Reglamento Interno de Trabajo y la Directiva que regula el Régimen Especial de Contratación Administrativa de Servicios - CAS en la Zona Registral N° IX - Sede Lima.
- Para la evaluación de Practicantes, la URH debe seguir los lineamientos establecidos en la normativa legal establecida para las Modalidades Formativas de Servicios en el Sector Público.

7.1.2. Términos y Condiciones de Empleo [ISO 27001 A.7.1.2]

a) Los contratos laborales deben incluir una sección en la cual se especifiquen las cláusulas de confidencialidad de la información.

b) El trabajador que incumpla estará sujeto a las acciones administrativas y disciplinarias que correspondan conforme a las normas vigentes en la materia.

7.2. DURANTE EL EMPLEO [ISO 27001 A.7.2]

7.2.1. Responsabilidades de gestión [ISO 27001 A.7.2.1]

Los servidores que ingresen a la Zona Registral N° IX - Sede Lima deben tener un proceso de inducción en el cual se brinden aspectos

relacionados de seguridad de la información, para que conozcan sus funciones y responsabilidades con respecto al Sistema de Gestión de Seguridad de la Información.

7.2.2. Conciencia de seguridad de información, educación y capacitación [ISO 27001 A.7.2.2]

a) Se debe desarrollar charlas de concientización y sensibilización a los servidores de la Zona Registral N° IX - Sede Lima, en las que se difundan los temas de protección de la información, su contribución a la eficacia del Sistema de Gestión de Seguridad de la Información incluyendo los beneficios de un mejor desempeño, las mismas que deben ser desarrolladas o gestionadas por el Oficial del SGSI en coordinación con la URH.

b) Las asistencias a las sesiones de concientización, sensibilización, educación y capacitación del Sistema de Gestión de Seguridad de la Información son de carácter obligatorio para el personal, y el responsable del cumplimiento será la URH.

c) Los servidores civiles deben conocer sus responsabilidades en temas relacionados con la seguridad de la información, a través de difusiones realizadas por la Unidad de Comunicaciones e Imagen Institucional – UCII.

7.2.3. Procesos disciplinarios [ISO 27001 A.7.2.3]

En caso de que el Oficial del SGSI identifique violaciones a las políticas y procedimientos relacionados con la seguridad de la información o el incumplimiento del literal n del artículo 124 del Reglamento Interno de Trabajo se debe proceder a ***informar al jefe inmediato para que imponga*** las sanciones disciplinarias indicadas en el artículo 135 del Reglamento Interno de Trabajo.

7.3. TÉRMINO Y CAMBIO DE EMPLEO [ISO 27001 A.7.3]

7.3.1. Término o cambio de las responsabilidades de empleo [ISO 27001 A.7.3.1]

a) La URH debe informar oportunamente los ceses de los servidores a las Unidades Orgánicas respectivas de la Zona Registral N° IX - Sede Lima que correspondan, para tomar las medidas preventivas y correctivas necesarias.

b) En cuanto al cambio de responsabilidades del empleo, es de responsabilidad del jefe de la Unidad Orgánica de origen y destino, informar oportunamente a la Unidad de Tecnologías de la Información - UTI sobre los perfiles y privilegios que se revocarán y otorgarán al personal para acceder a la red y los sistemas de información, para tomar las medidas preventivas y correctivas de acuerdo con sus métodos y procedimientos vigentes.

VIII. GESTIÓN DE ACTIVOS (ISO 27001-A.8)

8.1. RESPONSABILIDAD POR LOS ACTIVOS [ISO 27001 A.8.1]

8.1.1. Inventarios de activos [ISO 27001 A.8.1.1]

a) La Zona Registral N° IX - Sede Lima debe registrar y mantener actualizados los activos de información que están involucrados en el proceso parte del alcance del Sistema de Gestión de Seguridad de la Información en el documento “Formato de Inventario de Activos”, en el formato “Inventario de Licencias de Software” y en el formato “Listado de Programas de la Sunarp”.

b) Para el desarrollo del Inventario de Activos de Información se debe realizar lo especificado en el documento “Instructivo de Evaluación y Tratamiento de Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información”.

8.1.2. Propiedad de los activos [ISO 27001 A.8.1.2]

a) Todos los activos de información deben tener un “Propietario”, quien debe ser responsable de asegurar la apropiada clasificación y protección de los mismos; para lo cual, debe definir y revisar periódicamente las restricciones de acceso y las clasificaciones.

b) El propietario del activo de información se debe registrar en el Inventario de Activos de Información en el documento “Formato de Inventario de Activos”, según lo detallado en el documento “Instructivo de Evaluación y Tratamiento de Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información”.

c) Los Jefes de cada Unidad de Organización con la finalidad de descentralizar y mejorar la eficiencia en la administración de la seguridad de información delegará la propiedad de los activos de información a un servidor civil.

8.1.3. Uso aceptable de los activos [ISO 27001 A.8.1.3]

a) El uso de todos los activos de información deberá ser con el propósito expreso de realizar tareas relacionadas a las actividades de Zona Registral N° IX - Sede Lima.

b) Los activos de información deben ser utilizados adecuadamente cualquiera sea el medio que los soporte y el ambiente en que se procesen.

c) Ante la presencia de terceros en lugares públicos (ambientes de la entidad accesible a terceros), los servidores civiles no deben tratar información de manera presencial o telefónicamente temas sensibles que correspondan a información de uso interno y/o confidencial.

d) Los propietarios del activo de la información registral deben controlar que dicha información sea accedida únicamente por el personal de la Entidad debidamente autorizados y que cuente con los privilegios adecuados.

8.1.4. Retorno de activos [ISO 27001 A.8.1.4]

a) La finalización del empleo debe incluir el retorno previo de los activos de información proporcionados por Zona Registral N° IX - Sede Lima servidor civil o tercero (de ser el caso) para el desempeño de las funciones asignadas.

b) La devolución de los activos tecnológicos, así como la eliminación de la información contenida en los mismos se debe realizar en coordinación con el jefe inmediato y la UTI.

c) La entrega y retorno de activos deberá realizarse según lo indicado en el documento “Directiva para Normar la Entrega y Recepción de Cargo Aplicable al Personal de la Superintendencia Nacional de los Registros Públicos”.

8.2. CLASIFICACIÓN DE LA INFORMACIÓN [ISO 27001 A.8.2]

8.2.1. Clasificación de la Información [ISO 27001 A.8.2.1]

a) La información debe clasificarse según su sensibilidad o grado de impacto, según los niveles indicados en el documento “Instructivo de Evaluación y Tratamiento de Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información”.

b) Los propietarios de los activos de información deben ser responsables de la clasificación de la misma, en coordinación con el Oficial del SGSI, la clasificación se debe registrar en el Inventario de Activos de Información en el formato “Inventario de Activos”.

8.2.2. Etiquetado de la información [ISO 27001 A.8.2.2]

a) Teniendo en consideración los niveles de clasificación mencionados en el punto anterior, la Zona Registral N° IX - Sede Lima debe asegurarse que los activos de información definidos como “Confidencial” lleven un rótulo que identifique su nivel de clasificación.

b) El marcado o la rotulación de ***los activos de información se realiza de forma*** estandarizada ***para los activos que se encuentran en los sistemas de información y estos a su vez en servidores, se colocará*** una etiqueta roja ***en*** los activos físicos ***que los contenga. Para el caso de activos electrónicos que no se encuentren almacenados en los servidores se les colocará un pie de página “confidencial” como, por ejemplo: “Matriz de Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información”***

8.2.3. Manejo de activos [ISO 27001 A.8.2.3]

a) Los propietarios de los activos de información serán los encargados de velar por el adecuado manejo de cada uno de los activos, estableciendo los niveles de protección que apliquen según su clasificación.

b) Los documentos clasificados como Confidenciales deben estar protegidos contra pérdida o robo.

c) Servidor civil es responsable de recoger inmediatamente los documentos que imprima en las impresoras asignadas, a fin de mantener la reserva de la información.

d) Las fotocopiadoras, escáneres o cualquier forma de tecnología de reproducción de la entidad deben ser utilizadas solo y exclusivamente por personas autorizadas.

e) Es responsabilidad de cada Unidad Orgánica el destruir las impresiones que ya no sirven y que contienen información confidencial usando algún mecanismo de eliminación segura de información.

f) Los servidores civiles no deben hacer uso de los servicios ofimáticos de la entidad para actividades que no guarden ningún tipo de relación directa con sus funciones.

8.3. MANEJO DE MEDIOS [ISO 27001 A.8.3]

8.3.1. Gestión de los medios removibles [ISO 27001 A.8.3.1]

a) Toda la información almacenada en medios removibles de Zona Registral N° IX - Sede Lima debe estar debidamente controlada en cuanto a su uso, transporte y almacenamiento.

b) Los puertos USB deberán estar bloqueados por defecto mediante la solución de antivirus, ***configuración del BIOS o los privilegios del directorio activo,*** siendo la Unidad Tecnologías de la Información responsable de este control. En el caso se requiera la habilitación de los puertos USB para el uso de los medios removibles, deberán ser solicitados formalmente siguiendo los lineamientos definidos en el documento “Procedimiento de Atención de Servicio de Mesa De Ayuda y Soporte a Usuarios”.

c) Está prohibido el uso no autorizado de Memorias USB, discos CD/DVD o cualquier otro dispositivo de almacenamiento removible, ajenos a la entidad. De ser necesario el acceso a USB o CD/DVD deberá ser autorizado por el jefe de su Unidad o Coordinador Responsable correspondiente. Así mismo los usuarios deben evitar el uso de programas no autorizados.

8.3.2. Disposición de medios [ISO 27001 A.8.3.2]

En el caso de disposición o reasignación ***de cualquier medio digital o computadora***, se debe eliminar de manera segura cualquier tipo de información contenida en los mismos a través del proceso realizado por Mesa de Ayuda***. Esta actividad se realizará en un plazo máximo de dos semanas, de ser necesario se remitirá un correo al servidor civil que tenía asignado el equipo para que brinde la conformidad de la eliminación.***

8.3.3. Transferencia de medios físicos [ISO 27001 A.8.3.3]

a) Cualquier información confidencial que se encuentre en un medio físico y deba ser trasladada desde la Zona Registral N° IX - Sede Lima a un sitio externo deberá ser transportada en forma segura y se deberá registrar en el Anexo N° 04 Orden de salida, reingreso y desplazamiento interno de bienes muebles patrimoniales de la “Directiva para la gestión de bienes muebles patrimoniales en el marco del Sistema Nacional de Abastecimiento”.

b) Para el almacenamiento de las copias de respaldo en sitios externos a la organización se deberá aplicar el “Procedimiento de Respaldo de la Información y Control de Copias de Seguridad – Backup”.

IX. CONTROL DE ACCESO (ISO 27001-A.9)

9.1. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO [ISO 27001 A.9.1]

9.1.1. Políticas de Control de Acceso [ISO 27001 A.9.1.1]

a) La Zona Registral N° IX - Sede Lima debe establecer la presente Política de Control de Acceso:

- El control de acceso a los sistemas de información debe realizarse por medio de códigos de identificación y contraseñas únicos para cada servidor civil.
- Cada servidor civil (o grupo de servidores civiles) debe contar con un identificador de usuario (o de grupo) y una contraseña conocida sólo por dicho servidor civil (o grupo), mediante los cuales tendrá acceso a los sistemas de información autorizados, de acuerdo al perfil asignado por su Unidades Orgánicas.
- El nivel de acceso a un sistema de información se otorgará de acuerdo a:
  - Funciones del servidor civil.
  - Perfiles de acceso estandarizados.
  - Solicitud, autorización y administración de acceso.
  - Segregación de funciones.
  - Revisión periódica.
- Los sistemas de información, según su criticidad y uso, deberían desconectar automáticamente las sesiones de conexión tras un periodo definido de inactividad que sea configurable por cada sistema.
- Los sistemas de información críticos deben estar conectados en ambientes, entornos informáticos y/o segmentos de red aislados.
- Cuando el sistema de información crítico se ejecute en entornos compartidos, se debe identificar los sistemas con los que compartan recursos.
- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información debe ser asignado de acuerdo a la identificación previa de los requisitos de seguridad que se definan por los propietarios de los activos de información, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.
- Los equipos de cómputo deben ser asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
- ***Se debe controlar el acceso físico a los centros de datos.***

9.1.2. Acceso a redes y servicios de red [ISO 27001 A.9.1.2]

a) Los perfiles de acceso deben considerar los servicios de red y conexiones a las redes a los que un servidor civil puede tener acceso.

b) Se debe considerar la verificación de los medios usados para el acceso a los servicios de red.

c) Se deben implementar mecanismos de identificación de un servidor civil que se conecta remotamente a la red de la organización, así como la identificación del punto de conexión remota a través de la VPN y el perfil de los servidores civiles debe mantenerse durante las conexiones remotas a determinado sistema o servicio.

d) Para la conexión de equipos a la red se debe considerar:

- Limitar y registrar el número de intentos fallidos de conexión, luego de lo cual el servidor civil debe quedar deshabilitado por un periodo de tiempo.
- Limitar el tiempo de la conexión, luego del cual el servidor civil deberá autenticarse nuevamente.
- Contar con identificadores ***de usuarios*** que se conectan a la red.

e) Las actividades asociadas al alta, baja y modificación de usuarios de los sistemas informáticos se deben realizar según lo establecido en el documento “Procedimiento para la Creación del Identificador de Usuario, Contraseña, Asignación de Privilegios y Perfiles para la Baja de Usuarios de los Sistemas y Computadoras”

f) Bajo ninguna circunstancia debe manipularse el contenido de un determinado directorio con fines ajenos a los estrictamente laborales ni hacer uso indiscriminado de este sin la debida autorización del propietario del activo de la información.

g) Los directorios creados deben ser visibles solo a los servidores civiles que se les está permitido su acceso, con los niveles de lectura y/o escritura asignados. Bajo ninguna circunstancia deben ser mostrados abiertamente dentro del árbol de directorios del servidor que lo alberga sin una justificación de por medio.

9.2. GESTIÓN DE ACCESO DE USUARIO [ISO 27001 A.9.2]

9.2.1. Registro y cancelación de registro de usuarios [ISO 27001 A.9.2.1], Provisión del acceso de usuario [ISO 27001 A.9.2.2], Gestión de la información de autenticación secreta de los usuarios [ISO 27001 A.9.2.4], Remoción o ajuste de derechos de acceso [ISO 27001 A.9.2.6]

a) La solicitud y registro de usuarios y cuentas se realizará de acuerdo a los lineamientos establecidos en el “Procedimiento para la Creación del Identificador de Usuario, Contraseña, Asignación de Privilegios y Perfiles para la Baja de Usuarios de los Sistemas y Computadoras”.

b) Cada usuario de los sistemas de información de Zona Registral N° IX - Sede Lima deberá contar con:

- Identificador o Nombre de usuario que corresponde a la identidad de la persona y es único dentro de la red y de la aplicación.
- Password o contraseña que debe ser conocido sólo por el servidor civil.

c) La creación, modificación o deshabilitación de las cuentas realizará de acuerdo a los lineamientos establecidos en el "Procedimiento para la Creación del Identificador de Usuario, Contraseña, Asignación de Privilegios y Perfiles para la Baja de Usuarios de los Sistemas y Computadoras".

d) Cuando se elimine un identificador de usuario, no se debe volver a asignar a otra persona en el futuro.

e) En los casos de ceses, vacaciones, licencias de los trabajadores, los permisos y accesos a los sistemas de información deben ser retirados o bloqueados.

f) En los casos de cambio de responsabilidades del empleo, es de responsabilidad del jefe de la Unidad Orgánica ***o coordinador responsable*** del área de origen y destino, informar oportunamente a la UTI sobre los perfiles y privilegios que se revocarán y otorgarán al personal para acceder a la red y los sistemas de información, siguiendo los pasos indicados en el "Procedimiento para la Creación del Identificador de Usuario, Contraseña, Asignación de Privilegios y Perfiles para la Baja de Usuarios de los Sistemas y Computadoras"

9.2.2. Gestión de derechos de acceso privilegiados [ISO 27001 A.9.2.3]

Los usuarios administradores con sus respectivas contraseñas de cada uno de los sistemas informáticos involucrados en la operación, considerados críticos para la entidad y en particular sobre el control de acceso lógico a plataformas y sistemas de red serán creadas y resguardadas según el documento "Procedimiento de gestión de usuarios con perfil administrador".

9.2.3. Revisión de derechos de acceso de usuarios [ISO 27001 A.9.2.5]

El Oficial del SGSI de la Zona Registral N° IX - Sede Lima debe revisar periódicamente los derechos de acceso, revocando los que hayan caducado o ya no correspondan con la función desempeñada por cada servidor civil.

9.3. RESPONSABILIDADES DE USUARIO [ISO 27001 A.9.3]

9.3.1. Uso de información de autenticación secreta [ISO 27001 A.9.3.1], Sistema de gestión de contraseña [ISO 27001 A.9.4.3]

a) La contraseña de los servidores civiles para el acceso a los sistemas informáticos, plataformas y sistemas de red debe tener las siguientes características:

- Secreta y no compartida.
- Fácil de recordar, difícil de adivinar.

- Longitud mínima de 8 caracteres y máxima de 14 y deberá estar conformada por letras mayúsculas, minúsculas, números y/o caracteres especiales alfanuméricos.
- No se deben repetir contraseñas hasta por lo menos las 5 anteriores.
- Las cuentas deberán de quedar bloqueadas luego del tercer intento errado de una contraseña.
- Las contraseñas deben ser forzadas a cambiarse periódicamente, pudiendo considerar la criticidad de la aplicación, perfil de usuario y uso.
- Las contraseñas temporales o por defecto deben ser enviadas a los servidores civiles de manera directa, las cuales deben ser cambiadas inmediatamente por los mismos una vez recibidas y verificadas.
- De ser factible, la red y los sistemas de información de manera automática deberán forzar el cambio de la contraseña temporal de forma inmediata, en su defecto los servidores civiles deben cambiar inmediatamente la clave de acceso a la red y a los sistemas de información
- Los servidores civiles deben cambiar sus contraseñas asignadas en caso tengan sospecha de su conocimiento por parte de otra persona, y deben notificar del hecho a Mesa de ayuda o al Oficial del SGSI de la Zona Registral N° IX - Sede Lima
- No se deben usar contraseñas que solo sean palabras (aunque sean extranjeras), nombres y/o apellidos (del servidor civil, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares u otro relacionado), ni contraseñas completamente numéricas con algún significado (teléfono, DNI, fecha de nacimiento, otros).
- No se deben incluir las contraseñas en ningún mecanismo automático de conexión que las deje almacenadas en el equipo.

b) La contraseña de los usuarios administradores para el acceso a los sistemas informáticos, plataformas y sistemas de red debe tener las características indicadas en el “Procedimiento de gestión de usuarios con perfil administrador”.

9.4. CONTROL DE ACCESO DE APLICACIÓN Y SISTEMA [ISO 27001 A.9.4]

9.4.1. Restricción de acceso a la información [ISO 27001 A.9.4.1]

La Zona Registral N° IX - Sede Lima debe establecer que los servidores civiles tendrán derecho a acceder a la información según el perfil de usuario asignado y el nivel de clasificación de dicha información. En la generación de perfiles, se debe controlar los derechos de acceso a lectura, escritura, borrado y ejecución, según el documento “Procedimiento para la Creación del Identificador de Usuario, Contraseña, Asignación de Privilegios y Perfiles para la Baja de Usuarios de los Sistemas y Computadoras”

9.4.2. Procedimientos seguros de inicio de sesión [ISO 27001 A.9.4.2]

a) Para iniciar sesión en cualquiera de los sistemas informáticos, plataformas y sistemas de red, todos los servidores civiles deberán ingresar el usuario asignado y su respectiva contraseña.

b) Los servidores civiles de los sistemas informáticos, plataformas y sistemas de red que tengan un usuario asignado con su respectiva contraseña, no deberán compartir su usuario ni deberán hacerlo público.

c) Los servidores civiles deberán proteger el acceso a su máquina activando el protector de pantalla o bien haciendo un logout del sistema, adicionalmente se debe tener mecanismos automatizados que permitan realizar el logout de manera automática luego de un periodo de inactividad ***de 5 minutos.***

d) De acuerdo al nivel de criticidad y sensibilidad de la información administrada por un servidor civil, se podrán utilizar métodos de autenticación alternativa a las contraseñas, tales como tarjetas inteligentes, tokens o medios biométricos.

e) Los sistemas informáticos, plataformas y sistemas de red deberán registrar la fecha y hora del anterior inicio de sesión con éxito, así como los detalles de cualquier intento de inicio de sesión sin éxito.

9.4.3. Uso de programas de utilidad privilegiada [ISO 27001 A.9.4.4]

En la Zona Registral N° IX - Sede Lima se debe restringir y controlar estrechamente el uso de programas utilitarios que pudieran ser capaces de anular los controles del sistema y las aplicaciones, ***la que se realizará a través de otros programas utilitarios como por ejemplo el antivirus.***

X. CRIPTOGRAFÍA (ISO 27001-A.10)

10.1. CONTROLES CRIPTOGRÁFICOS [ISO 27001 A.10.1]

10.1.1. Política sobre el uso de controles criptográficos [ISO 27001 A.10.1.1], Gestión de claves [ISO 27001 A.10.1.2]

a) La Zona Registral N° IX - Sede Lima debe establecer la presente Política sobre el Uso de Controles Criptográficos:

- Se deberán utilizar controles criptográficos cuando se realice la copia de respaldo de la información de los servidores y bases de datos, para resguardar la información de manera segura y que solo pueda ser desencriptada por el especialista responsable.

b) Las claves de las encriptaciones realizadas deberán ser conocidas solo por el especialista responsable y el jefe de la UTI, siguiendo lo indicado en el documento “Procedimiento de Respaldo de la Información y Control de Copias de Seguridad – Backup”.

XI. SEGURIDAD FÍSICA Y AMBIENTAL (ISO 27001-A.11)

11.1. ÁREAS SEGURAS [ISO 27001 A.11.1]

11.1.1. Perímetro de seguridad física [ISO 27001 A.11.1.1], Controles de entrada física [ISO 27001 A.11.1.2], Seguridad de oficinas, salas e instalaciones [ISO 27001 A.11.1.3]

a) La Zona Registral N° IX - Sede Lima debe establecer que los entornos de almacenamiento de información deben tener un perímetro físico con un nivel de seguridad de acuerdo a su clasificación.

b) Todos los servidores civiles, cualquiera sea su condición contractual, que desee ingresar a las oficinas de la Zona Registral N° IX - Sede Lima, deberá de hacer uso de la credencial entregada (fotocheck), la misma que deberá mostrarse y permanecer en un lugar visible al ingreso y en todo momento que se encuentre dentro de las Oficinas de la Zona Registral N° IX - Sede Lima.

c) Para el personal contratado para servicios específicos y/o personal dedicado a proyectos que no poseen fotocheck, deberán presentar un documento que autorice su ingreso a las instalaciones.

d) Para las personas que visiten las instalaciones de la entidad, deberán identificarse con el respectivo documento de identidad e indicar el nombre y cargo de la persona que desea visitar; previo a su ingreso, el personal de seguridad y vigilancia, solicitará autorización para revisar las maletas, maletines, bolsos, carteras, cajas, etc. y preguntará a los visitantes si portan equipamiento tecnológico, como laptop, tableta, disco duro externo, los cuales serán registrados y anotados en el cuaderno de control respectivo. En ese sentido, el personal visitante se hace responsable por las acciones inapropiadas que perjudiquen a la entidad, en el momento de ingreso, si el personal visitante niega que porta equipamiento tecnológico y posteriormente se identifica la presencia de dicho equipamiento, se procederá a la comunicación al Unidades Orgánicas de Seguridad Física, para realizar la inmovilización, dada la advertencia al ingreso y se tomarán las acciones que resulten necesarias según informe que emita la Unidad de Asesoría Jurídica.

e) No se debe permitir el ingreso de personal interno y terceros, sin las autorizaciones correspondientes o que no sigan el procedimiento adecuado.

f) Los servidores civiles de la Zona Registral N° IX - Sede Lima no deben permitir que personas desconocidas o no autorizadas atraviesen las puertas u otras entradas con control físico de acceso, al mismo tiempo en que lo hacen ellos, evitando de esa forma su identificación y autenticación.

g) Los sistemas críticos que manejen información de la Zona Registral N° IX - Sede Lima deben estar en entornos restringidos, aislados de los usuarios comunes y deben tener controles de acceso físico y lógico seguros.

h) En lo posible, las oficinas deben quedar cerradas cuando no hay personas en su interior.

i) Al dejar momentáneamente el sitio de trabajo o al finalizar la jornada, los escritorios y los entornos de trabajo deben quedar desprovistos

de documentos críticos. Estos deben quedar bajo llave en archivadores, credenzas, cajones u otros medios seguros.

11.1.2. Protección contra amenazas externas y ambientales [ISO 27001 A.11.1.4]

a) Las Unidades Orgánicas deben contar con equipos apropiados de seguridad física para evitar en la Zona Registral N° IX - Sede Lima el daño ocasionado por desastres naturales o causados por el hombre.

b) La Zona Registral N° IX - Sede Lima debe contar con Certificado de Protocolo de Prueba de Puesta de Tierra y Certificado de Inspección Técnica de Seguridad en Defensa Civil actualizados.

c) Los materiales peligrosos e inflamables se deben almacenar distantes a las oficinas de tratamiento de información.

d) El centro de datos debe contar con un sistema de extinción de incendios, alarma de temperatura, alarma de detección de aniego, aire acondicionado y luces de emergencia.

e) Las oficinas de tratamiento de información crítica no deben ser ubicadas en zonas del edificio vulnerables al ingreso de extraños o a desastres en instalaciones colindantes o a desastres naturales.

11.1.3. Trabajo en zonas seguras [ISO 27001 A.11.1.5]

a) Sin perjuicio de la Ley Nº 28705 para la prevención y control de los riesgos del consumo del tabaco, los servidores civiles no deben fumar o ingerir alimentos o bebidas, cuando se encuentren frente al teclado o cerca a orificios o rejillas de ventilación de los equipos ***o cerca a detectores de humo***. El jefe de la Unidad Orgánica deberá verificar el cumplimiento del presente ítem.

b) No se debe proveer información sobre la ubicación del Gabinete de Cómputo o de los entornos restringidos, como mecanismo de seguridad.

c) El acceso a las oficinas de acceso limitado y restringido debe ser autorizado por los Jefes de las Unidades Orgánicas respectivas y supervisadas continuamente.

11.1.4. Zonas de entrega y de carga [ISO 27001 A.11.1.6]

a) La carga y descarga de activos debe realizarse únicamente por personal autorizado e identificado, el cual debe ser custodiado permanentemente por el responsable de la entrega o recepción.

b) Las tareas de carga y descarga se realizarán en el área física destinada para tal fin, que se encuentra junto al lado de la puerta de acceso al personal. Si se requiere del acceso a las oficinas internas, limitadas o restringidas, el jefe de la Unidad Orgánica respectiva debe autorizar, supervisar y comunicar dicho acceso al agente de seguridad de turno.

11.2. EQUIPOS [ISO 27001 A.11.2]

11.2.1. Ubicación y protección del equipamiento [ISO 27001 A.11.2.1]

a) La Zona Registral N° IX - Sede Lima debe establecer que todos los equipos de hardware y software que se utilicen para el tratamiento de información de la organización deben contar con las medidas de protección eléctrica y de comunicaciones para evitar daños a la información procesada.

b) El Data Center deberá contar con un mecanismo de protección eléctrica, de manera que se pueda interrumpir el suministro de energía en caso de emergencia.

c) Se deben monitorear las condiciones ambientales como temperatura y humedad, que puedan afectar negativamente la operatividad de los equipos del Data Center.

d) No se deberá mover o reubicar ningún equipo de cómputo, ya sea en forma parcial o en su totalidad, sin la previa coordinación y aprobación del jefe de la Unidad Orgánica y control patrimonial, la instalación o desinstalación debe ser solicitada a la UTI.

e) Los equipos de procesamiento de información crítica deben ser protegidos instalándolos en áreas de acceso limitado o restringido.

11.2.2. Servicios de suministro [ISO 27001 A.11.2.2]

a) Se debe contar con dispositivos de soporte físico que permitan un óptimo, continuo y seguro funcionamiento de los equipos de cómputo, tales como aire acondicionado, UPS (Uninterruptable Power Supply, en español, Sistema de Alimentación Ininterrumpida), estabilizadores, alarmas u otros; de acuerdo a su nivel de clasificación.

b) Los dispositivos de soporte físico deben ser probados periódicamente para asegurar un correcto funcionamiento, se deberán de probar cada vez que se realice el mantenimiento preventivo, el cual se realizará como mínimo una vez al año.

11.2.3. Seguridad del cableado [ISO 27001 A.11.2.3]

a) La Zona Registral N° IX - Sede Lima debe asegurar que todos los equipos de comunicaciones y cableado para el transporte de información, estarán protegidos de daños o interferencias que puedan afectar la integridad y disponibilidad de la información.

b) El cableado de telecomunicaciones debe seguir las normas y estándares internacionales correspondientes que garanticen el funcionamiento eficiente de la red.

11.2.4. Mantenimiento de los equipos [ISO 27001 A.11.2.4]

a) El mantenimiento de equipos de cómputo, aplicaciones y software es de exclusiva responsabilidad de la UTI.

b) El personal de la UTI debe llevar un registro global del mantenimiento efectuado sobre los equipos y sus cambios realizados desde su instalación.

c) Solo el personal de la UTI puede abrir y manipular los equipos de cómputo y la instalación de partes o piezas dentro de los equipos de cómputo.

d) El mantenimiento preventivo de equipos informáticos o dispositivos de soporte físico debe ser oportunamente comunicado y se deberá de tener un cronograma comunicado a las partes interesadas.

11.2.5. Retiro de los activos [ISO 27001 A.11.2.5]

La Zona Registral N° IX - Sede Lima debe establecer que los servidores civiles que requieran retirar activos físicos fuera de las oficinas de trabajo, deberán registrar en el Anexo N° 04 “Orden de salida, reingreso y desplazamiento interno de bienes muebles patrimoniales” según la “Directiva para la gestión de bienes muebles patrimoniales en el marco del Sistema Nacional de Abastecimiento”.

11.2.6. Seguridad de los equipos y de los activos fuera de las instalaciones [ISO 27001 A.11.2.6]

a) Todos aquellos equipos de computación (computadores portátiles, etc.) o medios magnéticos que por motivos circunstanciales son utilizados fuera de la entidad, no deben salir de la Zona Registral N° IX - Sede Lima sin una autorización formal previa, para lo cual se deberá registrar en el Anexo N° 04 “Orden de salida, reingreso y desplazamiento interno de bienes muebles patrimoniales” según la “Directiva para la gestión de bienes muebles patrimoniales en el marco del Sistema Nacional de Abastecimiento”.

b) Los equipos y medios que contengan información de la organización no deben ser desatendidos cuando estén fuera de las instalaciones.

11.2.7. Seguridad en eliminación o reutilización de equipos [ISO 27001 A.11.2.7]

Todos los equipos que son operados en la Zona Registral N° IX - Sede Lima, que contengan medios de almacenamiento deben revisarse para asegurar que todos los datos sensibles y software licenciado se haya eliminado de forma segura antes de su eliminación o reutilización. ***Asimismo, cuando son retirados por terceros del sitio de instalación por motivo de cambios, reparación o destrucción***.

11.2.8. Equipos de usuarios no atendidos [ISO 27001 A.11.2.8]

a) Al dejar un equipo desatendido temporalmente, el servidor civil debe bloquear el acceso a su PC/laptop y/o servidores, independientemente del tiempo que permanezcan alejados. Adicionalmente los equipos informáticos deberán estar configurados para que se bloqueen luego de cierto tiempo de inactividad ***(5 minutos).***

b) Al terminar la jornada de trabajo se debe apagar el equipo, siempre y cuando no se encuentren ejecutándose procesos programados ***o estén autorizados para ingresar por VPN*** y respondan a labores propias del cargo del servidor civil.

c) Se debe cerrar la sesión de administrador u ***operador*** de los servidores cuando se ha concluido con la labor.

11.2.9. Política de escritorio y pantalla limpia [ISO 27001 A.11.2.9]

La Zona Registral N° IX - Sede Lima debe establecer la presente Política de Escritorio y Pantalla Limpia:

a) La información confidencial almacenada de manera electrónica debe estar protegida de accesos no autorizados, especialmente cuando no estén en uso, ***por lo que se cuenta con un protector de pantalla que se activa cada 5 minutos.***

b) Una vez finalizada la tarea diaria, los servidores civiles no deben dejar hojas y papeles de trabajo sobre los escritorios con información ***confidencial.*** Asimismo, no deben dejar medios de almacenamiento donde se pueda obtener información de la organización. El almacenamiento de estos elementos se debe realizar preferiblemente en gabinetes bajo llave.

c) Se debe tener especial cuidado con el uso de dispositivos como fotocopias e impresoras de manera que el material con información confidencial no permanezca en ellas sin atención.

XII. SEGURIDAD DE OPERACIONES (ISO 27001-A.12)

12.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES [ISO 27001 A.12.1]

12.1.1. Procedimientos de operación documentados [ISO 27001 A.12.1.1]

a) Se debe identificar qué actividades del trabajo deben ser documentados con el fin de asegurar el mantenimiento y operación del Sistema de Gestión de Seguridad de la Información.

b) La creación y actualización de la información documentada se realizará de acuerdo a los procesos que se realizan en la Zona Registral N° IX - Sede Lima y deberán seguir las actividades y lineamientos definidos en el “Procedimiento de Gestión de Documentos de Soporte a los Procesos”.

12.1.2. Gestión de cambio [ISO 27001 A.12.1.2] *[ISO 27001 A.12.1.4]*

Todos los cambios en los sistemas de información, instalaciones de procesamiento o software base se deben realizar de acuerdo a los lineamientos respectivos de instalación, operación y mantenimiento, que permita identificar, registrar y controlar dichos cambios asegurando que no afectarán la disponibilidad e integridad de la información. Estos cambios deben realizarse mediante los lineamientos definidos en el “Procedimiento de Atención de Servicio de Mesa de Ayuda y Soporte a Usuarios”, “Procedimientos de Desarrollo, Mantenimiento y Seguridad de Programas” ***y las solicitudes que se realizan a través del Sistema de Gestión Documental***, los cuales deben contemplar que los cambios sean autorizados, notificados oportunamente y aprobados. Asimismo, que los entornos de pruebas y operación estén separados para reducir los riesgos de acceso no autorizado o cambios.

12.1.3. Gestión de capacidad [ISO 27001 A.12.1.3]

a) La UTI la Zona Registral N° IX - Sede Lima deberá proyectar y asegurar las demandas de capacidad de almacenamiento y procesamiento de información para evitar bajo desempeño de los sistemas o perder información por el mal uso de los recursos informáticos actuales.

b) Se debe monitorear el uso de los recursos críticos para identificar y evitar mal uso, y problemas de mala configuración o de congestión en la red.

c) La gestión de la capacidad debe realizarse según los lineamientos especificados en el documento “Procedimiento de Gestión de la Capacidad de los recursos informáticos”.

12.2. PROTECCIÓN DE MALWARE [ISO 27001 A.12.2]

12.2.1. Control Contra Malware [ISO 27001 A.12.2.1]

a) La Zona Registral N° IX - Sede Lima debe establecer la presente Política de Control Contra Malware:

- Los programas de detección de virus deben ser originales, estar instalados en todas las computadoras y servidores (equipos tecnológicos) de propiedad de la institución y configurados en las modalidades de protección en tiempo real y de análisis por demanda, para la detección y eliminación de archivos ejecutables o documentos que fuesen potencialmente peligrosos para el sistema operativo a causa de virus informáticos o malware.
- Los programas adquiridos para la detección de virus, deben ser actualizados automáticamente con las últimas actualizaciones de virus o malware existentes.
- Los servidores, al igual que las estaciones de trabajo, deberán tener instalado y configurado correctamente un software antivirus actualizable y activada la protección en tiempo real.
- No se debe descargar, instalar o tratar de instalar software no autorizado en los equipos de la Zona Registral N° IX - Sede Lima, salvo el personal de la UTI que por la naturaleza de sus funciones así lo requieran.
- No se debe ingresar a páginas web inseguras desde la red de la Zona Registral N° IX - Sede Lima.
- En caso un servidor civil detecte código malicioso en un equipo, debe informar inmediatamente a mesa de ayuda para que tome las medidas necesarias.

12.3. BACKUP [ISO 27001 A.12.3]

12.3.1. Backup [ISO 27001 A.12.3.1]

a) La frecuencia de las copias de respaldo debe establecerse de manera conjunta con los propietarios del activo de la información en base a criterios como tipo (información, software y sistemas), criticidad, volumen entre otros y que reflejen las necesidades de la entidad.

b) Toda información resguardada en medios deberá almacenarse en lugares que cumplan con máximas medidas de protección. Tales medidas deben incluir su resguardo adecuado y el sitio debe contar con mecanismos de detección de humo, calor y humedad y control de acceso físico.

c) Toda información crítica contenida en medios debe almacenarse además en otra instalación fuera del ambiente del edificio donde normalmente residen los resguardos de esa información que se realizan periódicamente. El sitio externo donde se resguardan dichas copias, debe contar con controles de seguridad física y además contar con los mecanismos de detección de humo, calor y humedad y control de acceso físico.

d) El respaldo y restauración de información se debe realizar según los lineamientos definidos en el documento "Procedimiento de Respaldo de la Información y Control de Copias de Seguridad – Backup".

12.4. REGISTRO Y MONITOREO [ISO 27001 A.12.4]

12.4.1. Registro de eventos [ISO 27001 A.12.4.1]

a) Las aplicaciones de la Zona Registral N° IX - Sede Lima deben contar con la capacidad de registrar los eventos de seguridad y permitir el monitoreo de accesos indebidos e intrusiones, registrando el usuario, fecha, hora y última acción realizada.

b) Para todo sistema que maneje información confidencial de la Zona Registral N° IX - Sede Lima se debe evaluar la generación de logs que almacenen información, sea en base de datos o en registros de los servidores, sobre actividades de los servidores civiles, activaciones y desactivaciones de los sistemas y eventos de seguridad de información, los cuales deben ser guardados por lo menos durante un mes, para asistir futuras investigaciones y para el monitoreo de control de acceso.

12.4.2. Protección de información de registro [ISO 27001 A.12.4.2]

a) La Zona Registral N° IX - Sede Lima debe establecer que todos los logs que se registren deben mantenerse en forma confidencial de manera tal que no puedan ser leídos por personas que no estén autorizadas para tal efecto y deben contar con privilegios de solo lectura. Se deben poder revisar estos logs cada vez que un incidente de seguridad de la información lo requiera o bien dentro de los procesos de revisión periódica de auditoría.

b) El Oficial del SGSI debe realizar supervisiones de manera periódica para revisar el cumplimiento de este control.

12.4.3. Registros de administrador y operador [ISO 27001 A.12.4.3]

a) Para la generación de los registros de auditoría deben tener en cuenta los siguientes lineamientos:

- Se debe registrar la actividad de los administradores y operadores del sistema; identificando a la persona, hora de ingreso y acciones realizadas.

- Las actividades diarias no deben realizarse a través de cuentas con accesos privilegiados.
- Toda cuenta con acceso de administrador debe poseer un responsable directo.

b) El Oficial del SGSI debe realizar supervisiones de manera periódica para revisar el cumplimiento de este control.

12.4.4. Sincronización de reloj [ISO 27001 A.12.4.4]

Todos los relojes de los sistemas de procesamiento de información de la Zona Registral N° IX - Sede Lima deben estar sincronizados con una fuente de tiempo exacta convenida, con el fin de obtener un control apropiado para la determinación exacta de eventos no deseados en la infraestructura de red o para la investigación efectiva de incidentes de seguridad de la información.

12.5. CONTROL DE SOFTWARE EN LA PRODUCCIÓN [ISO 27001 A.12.5]

12.5.1. Instalación de software en sistemas operacionales [ISO 27001 A.12.5.1]

a) La Zona Registral N° IX - Sede Lima debe establecer que existan controles para asegurar que los cambios o actualizaciones de los sistemas informáticos no provoquen errores de procesamiento de información y evitar la pérdida de integridad de los datos.

b) La descarga de actualizaciones del sistema operativo de las PC se realizará a través de un único servidor en el cual se instale el servicio correspondiente, a fin de no generar flujos de transmisión que degraden la red.

c) La actualización de software de producción, aplicaciones y bibliotecas de programas debe implementarse ***según el "Procedimiento de Desarrollo, Mantenimiento y Seguridad de Programas"***

d) Cuando se requiera la instalación de un software, se deberá seguir los lineamientos definidos en el "Procedimiento de Atención de Servicio de Mesa de Ayuda y Soporte a Usuarios".

12.6. GESTIÓN DE VULNERABILIDAD TÉCNICA [ISO 27001 A.12.6]

12.6.1. Gestión de vulnerabilidades técnicas [ISO 27001 A.12.6.1]

a) Se debe obtener de forma periódica información sobre las vulnerabilidades técnicas de los sistemas de información, evaluar su exposición a tales vulnerabilidades y tomar medidas para abordar el riesgo asociado.

b) Se debe contar con conocimiento y mantenerse actualizado las vulnerabilidades técnicas de los sistemas utilizados que permita identificar los riesgos asociados y tomar acciones preventivas.

c) El Oficial del SGSI debe monitorear y evaluar la gestión de las vulnerabilidades técnicas para asegurar su efectividad y eficiencia por lo menos una vez por año.

12.6.2. Restricciones en la instalación de software [ISO 27001 A.12.6.2]

a) La UTI es la única Unidad Orgánica autorizada para realizar instalación de software en la Zona Registral N° IX - Sede Lima.

b) Para todos los equipos de cómputo propiedad de la Zona Registral N° IX - Sede Lima, se debe instalar únicamente el software que cuente con licencia autorizada o software libre de uso autorizado para uso en la organización.

c) Si se detecta software que no cumpla con estos lineamientos se debe desinstalar de manera inmediata para garantizar el cumplimiento de la Ley sobre el Derecho de Autor.

12.7. CONSIDERACIONES PARA LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN [ISO 27001 A.12.7]

12.7.1. Controles de auditoría de sistemas de información [ISO 27001 A.12.7.1]

a) Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

b) Las auditorías y controles de seguridad a los sistemas informáticos deberán ser realizadas fueras del horario laboral.

c) Para la ejecución de estas auditorías, toda la información necesaria debe estar limitada y disponible para los auditores con permiso de solo lectura.

XIII. SEGURIDAD DE COMUNICACIONES (ISO 27001-A.13)

13.1. GESTIÓN DE SEGURIDAD DE REDES [ISO 27001 A.13.1]

13.1.1. Controles de redes [ISO 27001 A.13.1.1]

a) El uso de los recursos de red para el acceso a internet deberá ser utilizado con el propósito expreso de realizar tareas relacionadas a las actividades laborales.

b) Solo los responsables de los diversas Unidades Orgánicas pueden solicitar acceso para el personal a su cargo, en atención a las funciones y actividades que desempeña, a los diversos servicios de red.

c) Personal de la UTI debe habilitar y controlar los accesos a los servicios de red, monitorear la actividad de la red interna y desde/hacia Internet.

13.1.2. Seguridad de los servicios de redes [ISO 27001 A.13.1.2]

a) La UTI debe establecer que todos los sistemas y servicios de red están actualizados con los parches y recomendaciones de los fabricantes para asegurar los niveles óptimos de control y seguridad.

b) Los servicios de red deben contar con mecanismos de detección y eliminación de código malicioso.

c) Los accesos a la red internos y externos deben contar con mecanismos de seguridad perimetrales.

13.1.3. Separación en redes [ISO 27001 A.13.1.3]

La UTI debe controlar la seguridad de la red dividiéndola en dominios de red separados. Se deben implementar dominios o grupos de red necesarios para controlar los accesos lógicos a la red y flujos de información, teniendo en cuenta el impacto en el rendimiento de la red.

13.2. TRANSFERENCIA DE INFORMACIÓN [ISO 27001 A.13.2]

13.2.1. Políticas de transferencia de información [ISO 27001 A.13.2.1]

La Zona Registral N° IX - Sede Lima debe establecer la presente Política de Transferencia de Información:

- ***La información digital se transmitirá a través de redes digitales las cuales se encuentran protegidas mediante el Directorio Activo a la cual se accede mediante identificadores de usuario asignadas con las debidas autorizaciones según el "Procedimiento para la Creación del Identificador de Usuario, Contraseña, Asignación de Privilegios y Perfiles para la Baja de Usuarios de los Sistemas y Computadoras". El Directorio Activo, se encarga de proteger la información transmitida a través de la red de datos.***
- El intercambio manual ***de documentación registral como por ejemplo los títulos de inscripción que se remiten de una oficina a otra se efectúan a través de un servicio de transporte de documentos y paquetería, mediante paquetes que se aseguran con un precinto de seguridad.***
- ***Los documentos electrónicos presentados por las notarías a los Registros Públicos para la inscripción de títulos, presentados a través del Sistema de Intermediación Digital (SID), se protegen mediante la firma digital. Asimismo, el asiento y la anotación de inscripción remitidos a la notaría se protege mediante la firma digital del registrador.***

13.2.2. Acuerdos sobre transferencia de información [ISO 27001 A.13.2.2]

a) Todos los terceros ***que brindan servicios deben tener una cláusula de confidencialidad establecidos en los Términos de Referencia o en las Especificaciones Técnicas que se encuentran referidas en su contrato.***

b) ***Toda actividad que genere*** intercambio de información (clasificada como confidencial) con terceros o que afecte el principio de seguridad, deberá realizarse tomando en cuenta ***los niveles aceptables de control de acceso***.

13.2.3. Mensajería electrónica [ISO 27001 A.13.2.3]

a) La UTI debe ser el responsable por la creación de una cultura dentro de la organización acerca del buen uso del correo electrónico.

b) El correo electrónico es personal e intransferible, los servidores civiles son responsables de todas las actividades que se realicen por medio de la cuenta de correo electrónico que le sea asignada. Asimismo, es de uso exclusivo para las actividades que estén relacionadas con el cumplimiento directo de sus funciones.

c) El administrador del sistema de correo electrónico deberá mantener la privacidad, confidencialidad y seguridad de la información almacenada en el servidor de correo electrónico, el cual sólo podrá ser abierto, incautado, interceptado o intervenido por mandamiento motivado del juez.

d) Se deben utilizar diversas técnicas para prevenir el correo basura, entre ellos Antispam.

e) Los servicios de mensajería electrónica deberán cumplir con las regulaciones legales vigentes.

f) Los servidores civiles al enviar un correo electrónico deberán utilizar siempre el campo “asunto” o “subject” a fin de resumir el tema del mensaje.

g) Con respecto a la autofirma en el correo (Ejemplo: Nombre, cargo, teléfono, anexo), se recomienda que esta sea breve e informativa y que no ocupe más de tres líneas. No incluir la dirección de correo en la firma.

h) Todo correo electrónico externo no solicitado y/o recibido de fuentes desconocidas deberá inmediatamente eliminarse en forma definitiva del recipiente de correos recibidos por medidas de seguridad.

i) Todo usuario del sistema de correo electrónico podrá configurar un mensaje automático de respuesta por vacaciones en su cuenta de correo, un día antes del inicio de sus vacaciones.

13.2.4. Acuerdo de confidencialidad o de no divulgación [ISO 27001 A.13.2.4]

a) Luego de la aprobación del presente documento la totalidad de los nuevos contratos de los Servidores Civiles y practicantes deberán incluir cláusulas de Confidencialidad.

b) La vigencia de esta obligación de confidencialidad, deberá extender incluso hasta después del cese de la relación contractual o laboral con la organización.

XIV. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS (ISO 27001-A.14)

Nos encontramos excluidos de este objetivo de control, debido a que se realiza en la Sede Central.

XV. RELACIÓN CON PROVEEDORES (ISO 27001-A.15)

15.1. SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON LOS PROVEEDORES [ISO 27001 A.15.1]

15.1.1. Política de seguridad de información para la relación con los proveedores [ISO 27001 A.15.1.1]

La Zona Registral N° IX - Sede Lima debe establecer la presente Política de la Relación con los terceros, la cual debe ser incluida en las especificaciones técnicas, según sea el caso de servicios o bienes, respectivamente; debiendo considerar:

- Los contratos de los proveedores deben contener cláusulas / acuerdos de confidencialidad en sus contratos, dichas cláusulas / acuerdos deberán comprometerlos a no divulgar, usar o explotar la información de la organización a la cual tengan acceso.
- Los terceros deben registrar al momento de su entrada a la entidad, en el control de ingreso, el ingreso de equipos de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que sean de su propiedad.
- El servicio de tecnologías de información entregado por terceros según su criticidad e impacto en la continuidad del negocio, deben incluir parámetros de seguridad de información o Acuerdo de Nivel de Servicio dentro del contrato establecido y de ser el caso contemplar penalidades ante el incumplimiento, el nivel de servicio de los terceros debe ser evaluado y aceptado por la UTI.

15.1.2. Abordar la seguridad dentro de acuerdos con proveedores [ISO 27001 A.15.1.2] y Cadena de suministro de tecnología de información y comunicaciones [ISO 27001 A.15.1.3]

a) Las Unidades Orgánicas en coordinación con el Oficial del SGSI que requieren los bienes o servicios de terceros, deben definir en los términos de referencia los requisitos de seguridad de la información para asegurar que no haya malentendidos entre la organización y el proveedor respecto a las obligaciones de ambas partes.

b) De ser el caso, el jefe de cada Unidad Orgánica debe solicitar a la UTI, la asignación de accesos para las labores del tercero, a través del “Procedimiento para la Creación del Identificador de Usuario, Contraseña, Asignación de Privilegios y Perfiles para la Baja de Usuarios de los Sistemas y Computadoras”.

c) ***Los equipos de Tecnologías de la Información y Comunicaciones (TIC) al ser adquiridos, tienen que ser revisados y contar con el V°.B°. de la Unidad de Tecnologías de la Información. Asimismo, deben contar con garantía, mantenimiento preventivo y soporte técnico.***

15.2. GESTIÓN DE LA PRESTACIÓN DE SERVICIO [ISO 27001 A.15.2]

15.2.1. Monitoreo y revisión de los servicios de proveedores [ISO 27001 A.15.2.1]

a) Los servicios de terceros se deben monitorear y revisar de acuerdo a lo especificado en los términos de referencia, en la orden de servicio y/o en el contrato.

b) Se debe monitorear y revisar periódicamente los registros y reportes emitidos por los servicios de terceros, para verificar el cumplimiento de los parámetros de seguridad de información establecidos.

c) Los jefes de las Unidades Orgánicas deben comunicar las fallas e incidentes de seguridad de la información en los servicios de terceros.

15.2.2. Gestión de cambios de los servicios del proveedor [ISO 27001 A.15.2.2]

a) Se deberá mantener la operación de la Zona Registral N° IX - Sede Lima controlando el impacto de los servicios de terceros ante cambios regulados por la normatividad de contrataciones.

b) Se deben registrar todos los cambios y mejoras realizadas en los sistemas de comunicaciones u operaciones por servicios externos según la normatividad de contrataciones.

c) Se debe realizar la reevaluación de riesgos ante los cambios originados por las actividades del proveedor según lo precisado en el “Instructivo de evaluación y tratamiento Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información”.

XVI. GESTIÓN DE INCIDENTES DE SEGURIDAD DE INFORMACIÓN (ISO 27001-A.16)

16.1. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS [ISO 27001 A.16.1]

16.1.1. Responsabilidades y procedimientos [ISO 27001 A.16.1.1]

a) La Zona Registral N° IX - Sede Lima debe establecer un conjunto de procedimientos y responsabilidades para el manejo de eventos e incidentes de seguridad de la información con el fin de asegurar una respuesta efectiva, restablecer la operación del negocio y analizar las causas con fines de auditoría.

b) Los responsables de responder a eventos de seguridad de la información, así como los pasos a seguir para su atención se deben definir en el documento “Procedimiento de Gestión de Incidentes de Seguridad de Información”.

c) La UTI, a través de Mesa de Ayuda, brindará servicio a los servidores civiles ante el desconocimiento y/o problemas con el uso de las herramientas informáticas como: File server, Correo, Cambio de contraseñas, entre otros.

16.1.2. Informe de eventos de seguridad de información [ISO 27001 A.16.1.2]

Cualquier servidor civil debe poder reportar ***incidentes o eventos*** detectadas o sospechas que se tengan, según los lineamientos definidos en el documento “Procedimiento de Gestión de Incidentes de Seguridad de Información”, el cual deberá contemplar:

- Los eventos o incidentes de seguridad de información se reportarán oportunamente mediante correo electrónico o vía telefónica, a mesa de ayuda.
- Los sistemas de información deben contar con registros de eventos de seguridad, y en lo posible generar alertas.
- Todo incidente debe ser registrado e informado de su solución., de acuerdo a lo definido en el "Procedimiento de Gestión de Incidentes de Seguridad de la Información".

16.1.3. Informes de debilidades de seguridad de información [ISO 27001 A.16.1.3]

Las debilidades de seguridad de información deben ser reportadas por los servidores civiles a sus jefes inmediatos y los terceros a los responsables de la ejecución contractual, para de ser el caso se informe al Oficial del SGSI de la Zona Registral N° IX – Sede Lima.

16.1.4. Evaluación y decisión sobre los eventos de seguridad de información [ISO 27001 A.16.1.4]

Se deben evaluar los eventos de seguridad de la información y decidir si se clasifican como incidentes de seguridad de la información antes de su atención, lo cual se debe realizar según los lineamientos definidos en el documento "Procedimiento de Gestión de Incidentes de Seguridad de Información".

16.1.5. Respuesta a los incidentes de seguridad de información [ISO 27001 A.16.1.5]

Los incidentes de seguridad de la información deben responderse de acuerdo a lo definido en el documento Procedimiento de Gestión de Incidentes de Seguridad de Información. El cual debe contemplar:

- Considerar para incidentes mayores o disruptivos el "Procedimiento de Gestión de incidentes disruptivos" del "Plan de recuperación tecnológico ante desastres".
- Considerar para la solución de un evento: análisis de causa, contención, acciones correctivas, reporte a la jefatura, registros de auditoría. Asimismo, realizar un análisis forense de seguridad de información, de ser necesario.
- Cuando sea necesario, se deberá guardar evidencia del evento, para poder investigar las causas del mismo.
- Todas las medidas correctivas y acciones de emergencia deben ser documentadas y realizadas sólo por personal autorizado.
- Se debe mantener los contactos actualizados según su nivel de escalamiento al interno o con servicios dados por terceros.

16.1.6. Aprendiendo de los incidentes de seguridad de la información [ISO 27001 A.16.1.6]

Se deben registrar los incidentes ocurridos, tipos, causas, el impacto ocasionado y forma de resolución, con el objeto de tener estadísticas

anuales de comportamiento de respuesta ante incidentes, aprender de lo ocurrido y establecer mejoras en las acciones de control y las políticas de seguridad de la información cuando sea necesario; lo cual deberá realizarse según los lineamientos definidos en el documento "Procedimiento de Gestión de Incidentes de Seguridad de Información".

16.1.7. Recolección de evidencia [ISO 27001 A.16.1.7]

a) Se deben mantener las evidencias de los incidentes de seguridad de la información, lo cual se debe realizar según los lineamientos definidos en el documento "Procedimiento de Gestión de Incidentes de Seguridad de Información".

b) Deben establecerse todos los mecanismos de control para evidenciar toda acción maliciosa sobre información crítica perteneciente a la Zona Registral N° IX - Sede Lima. Toda actividad sospechosa de un servidor civil acerca del tratamiento de la información debe ser registrada en forma detallada para ser utilizada como evidencia y que permita la aplicación de sanciones acordes al impacto causado por dicha acción maliciosa.

c) Cuando una acción de seguimiento contra una persona u organización, después de un incidente de seguridad de información, implique acción legal, la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la colocación de evidencia en la jurisdicción relevante. Para ello los sistemas críticos deben cumplir con la producción de evidencia objetiva.

XVII. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (ISO 27001-A.17)

17.1. CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN [ISO 27001 A.17.1]

17.1.1. Planificación de la continuidad de seguridad de la información [ISO 27001 A.17.1.1]

La Zona Registral N° IX - Sede Lima debe asegurar la continuidad de las operaciones en caso de una contingencia no prevista con el fin de reducir el impacto en el negocio. Para ello debe existir un plan de contingencia debidamente documentado y administrado "en sitio" para el desarrollo y mantenimiento de los servicios informáticos de la Zona Registral N° IX - Sede Lima denominado Plan de Continuidad de Negocios el cual debe estar elaborado con base en los lineamientos y requerimientos de la seguridad de la información y debe estar sujeto a escalamiento y pruebas.

17.1.2. Implementación de la continuidad de seguridad de la información [ISO 27001 A.17.1.2]

a) La Zona Registral N° IX - Sede Lima cuenta con un Plan de Continuidad del Negocio, que permite hacer frente a contingencias y restablecer en el menor tiempo posible los servicios, disminuyendo el impacto que pueda tener para la entidad.

b) La implementación de la continuidad de seguridad de la información debe realizarse según los lineamientos definidos en el documento "Plan de Continuidad de Negocio".

17.1.3. Verificar, revisar y evaluar la continuidad de seguridad de la información [ISO 27001 A.17.1.3]

a) El Plan de Continuidad del Negocio debe recibir mantenimiento para que se encuentre actualizado al momento de ser probado y se encuentre alineado a la realidad de las operaciones en la organización.

b) Periódicamente se debe revisar y probar la efectividad del Plan de Continuidad de Negocios vigente. Estas pruebas deben consistir en la simulación de varios escenarios posibles de emergencias y lograr la recuperación de información en el menor tiempo posible, para lo cual se deberá de seguir lo indicado en el documento "Procedimiento de Ejercicios y Pruebas del Plan de Recuperación Tecnológica ante Desastres".

17.2. REDUNDANCIAS [ISO 27001 A.17.2]

17.2.1. Disponibilidad de instalaciones de procesamiento de información [ISO 27001 A.17.2.1]

La Zona Registral N° IX - Sede Lima deberá tener la redundancia suficiente para poder continuar con la disponibilidad de las instalaciones de procesamiento de información, a través de un sitio alterno.

XVIII. CUMPLIMIENTO (ISO 27001-A.18)

18.1. CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES [ISO 27001 A.18.1]

18.1.1. Identificación de la legislación aplicable y los requisitos contractuales [ISO 27001 A.18.1.1]

Se debe identificar, documentar, mantener y cumplir todos los requisitos legales, regulatorios y contractuales vigentes que pueden afectar a los sistemas de información de la Zona Registral N° IX - Sede Lima, para lo cual se deberá de verificar en las normas legales publicadas en El Peruano que son enviadas diariamente por correo electrónico a todos los servidores civiles y las alertas registrales con las normas que específicamente afectan las actividades registrales.

18.1.2. Derechos de propiedad intelectual [ISO 27001 A.18.1.2]

a) Se debe tener un inventario y control estricto respecto de la cantidad y vigencia de las licencias de software base (sistemas operativos), base de datos y aplicaciones comerciales utilizadas por la Zona Registral N° IX - Sede Lima. El no cumplimiento de este control puede traducirse en la utilización de software adquirido en forma ilegal que comprometa la imagen y perjudicar económicamente o legalmente a la organización. Adicionalmente, los contratos con terceros deben contemplar aspectos referidos a los derechos de propiedad intelectual.

b) Se deben archivar todas las licencias de software base (sistemas operativos), base de datos y aplicaciones comerciales adquiridas, a fin de que se encuentren disponibles en caso que sean requeridas por auditoría legal.

c) El Oficial del SGSI deberá revisar como mínimo 1 vez al año, los sistemas de información y estaciones de trabajo PC y laptops, a fin de verificar la no existencia de copias de software no licenciado. El servidor civil será responsable por el contenido de programas no autorizados en el disco duro de la computadora.

18.1.3. Protección de registros [ISO 27001 A.18.1.3]

a) Todos los registros de la entidad, incluyendo expedientes y documentos electrónicos deben ser protegidos y mantenidos adecuadamente hasta que sean necesarios y de acuerdo a lo establecido por requerimientos operativos, legales o contractuales.

b) El cronograma de retención de registros debe considerar como períodos o tiempos de retención, los plazos establecidos por las entidades reguladoras a nivel nacional.

c) Los registros no deben ser destruidos antes de culminado el periodo de retención establecido.

d) La Unidad Orgánica responsable de la retención de los registros físicos es el Archivo Central siguiendo lo indicado en el documento “Procedimiento de Administración de Archivo de la Zona Registral N° IX - Sede Lima”, y de los registros electrónicos es la UTI, según el caso, quienes en coordinación con los responsables de las unidades orgánicas definirán los periodos de retención para cada tipo de registros.

e) Los plazos de retención de registros deben ser revisados y actualizados cuando ocurran cambios en la normativa legal correspondiente, para garantizar que se mantiene vigente el esquema de clasificación y los requerimientos legales.

f) Una vez culminado el periodo de retención, los registros pueden ser eliminados de acuerdo a lo señalado en la normativa correspondiente.

g) Cada Unidad Orgánica debe adoptar mecanismos de protección necesarios para proteger los registros físicos o expedientes que se encuentran bajo su custodia.

h) La UTI deberá adoptar mecanismos de protección necesaria para proteger la integridad, disponibilidad y la confidencialidad de los registros electrónicos que se encuentran bajo su custodia.

18.1.4. Privacidad y protección de datos personales [ISO 27001 A.18.1.4]

a) La recolección de datos personales no puede hacerse por medios desleales, fraudulentos, en forma contraria a las disposiciones de ley o sin el consentimiento del titular o persona natural a la que están referidos.

b) Se deberá contar con los Documentos emitidos por la Autoridad Nacional de Protección de Datos Personales donde aceptan la inscripción de los bancos de datos personales.

c) Los datos personales deben utilizarse para los fines que han sido recolectados salvo que provengan o se hayan recolectado de fuentes accesibles al público según lo señalado en la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.

d) Todos los titulares de los datos personales podrán solicitar el uso de sus derechos ARCO, para lo cual se utilizara el formato "Solicitud para el ejercicio de derechos del titular de datos personales" tal como se encuentra indicado en el documento PR-026-JEF-ZRIX "Procedimiento de Atención de Solicitudes para el Ejercicio de Derechos del Titular de Datos Personales"

e) Los datos personales que revelan origen racial y étnico, convicciones políticas y religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual, sólo pueden ser recolectados y ser objeto de tratamiento cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que corresponden a sus titulares.

18.1.5. Regulación de controles criptográficos [ISO 27001 A.18.1.5]

Se debe contar con lineamientos que aseguren el cumplimiento de la normativa vigente relacionada a controles criptográficos aplicables a la organización.

18.2. REVISIONES DE SEGURIDAD DE LA INFORMACIÓN [ISO 27001 A.18.2]

18.2.1. Revisión independiente de seguridad de la información [ISO 27001 A.18.2.1]

a) El Oficial del SGSI o un auditor interno, deberá realizar una revisión anual como mínimo, del Sistema de Gestión de Seguridad de la Información para verificar la vigencia de los controles implementados.

b) El Coordinador del SGI debe coordinar con la Alta Dirección la realización de las revisiones de seguridad de la información, como mínimo una vez al año, efectuados por personal externo; salvo que medien razones fundadas relativas a un cambio reciente de los directivos de la Alta Dirección.

c) Las auditorías al Sistema de Gestión de Seguridad de la Información deberán realizarse siguiendo los lineamientos definidos en el "Procedimiento de auditorías internas del Sistema Integrado de Gestión".

18.2.2. Cumplimiento de las políticas y normas de seguridad [ISO 27001 A.18.2.2]

a) El Oficial del SGSI en conjunto con el Comité del Sistema Integrado de Gestión deben asegurar que todas las políticas, procedimientos y estándares definidos para la Zona Registral N° IX - Sede Lima son

cumplidas en su totalidad, las reuniones para tal fin deben quedar registradas en Actas de Reunión.

b) Los jefes de las Unidades Orgánicas deben asegurarse que se cumplan correctamente todos las políticas y procedimientos de seguridad de información, siendo los gestores directos en su área de responsabilidad y de informar oportunamente al Oficial del SGSI en caso de no cumplimiento.

c) Cualquier inquietud o duda que generase la aplicación o interpretación de estas políticas y normas debe ser consultada necesariamente al Oficial del SGSI.

18.2.3. Revisión de cumplimiento técnico [ISO 27001 A.18.2.3]

a) Todos los sistemas informáticos de la Zona Registral N° IX - Sede Lima deben ser verificados periódicamente para asegurar el cumplimiento de los niveles apropiados de seguridad, el Oficial del SGSI debe comprobar que se realice esta actividad.

CUADRO DE CONTROL DE CAMBIOS

Ítem	Descripción del cambio	Código / Versión
-	Elaboración inicial del documento.	MN-001-JEF-ZRIX / V.01
	Se agregó el término “Oportunidades” donde se mencione al Instructivo de evaluación y tratamiento Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información.	MN-001-JEF-ZRIX / V.02
VIII	Se modificó el literal a. del numeral 8.1.1. Inventarios de activos. Modificación en el literal b. e incorporación del literal c. del numeral 8.3.1. Gestión de los medios removibles.	
XII	Se agregaron precisiones al numeral 12.1.2. Gestión de cambio. Incorporación del 1er y 2do enunciado del numeral 12.2.1. Control contra Malware.	
III	Se agregaron precisiones en el numeral 3.4, 3.5 y 3.6.	MN-001-JEF-ZRIX / V.03
V	Se modificó el numeral 5.1.1. Política de seguridad de información, con respecto a la “Matriz de Comunicaciones”	
VI	Se modificaron y agregaron contenidos en los numerales: 6.1.4. Contacto con grupos de interés especial, 6.2.1. Política de dispositivo móvil y 6.2.2. Teletrabajo.	
VII	Se modificaron y agregaron contenidos en los numerales: 7.1.1. Selección y 7.2.3. Procesos disciplinarios.	
VIII	Se modificaron y agregaron contenidos en los numerales: 8.2.2. Etiquetado de la información, 8.3.1. Gestión de los medios removibles y 8.3.2. Disposición de medios.	
XI	Se modificaron y agregaron contenidos en los numerales: 11.2.7. Seguridad en eliminación o reutilización de equipos, 11.2.8. Equipos de usuarios no atendidos y 11.2.9. Política de escritorio y pantalla limpia.	
XII	Se modificaron y agregaron contenidos en los numerales: 12.1.2 Gestión de cambio y 12.5.1 Instalación de software en sistemas operacionales.	

XIII	Se modificaron y agregaron contenidos en los numerales: 13.2.1. Políticas de transferencia de información y 13.2.2. Acuerdos sobre transferencia de información	
XIV	Se agregó el numeral XIV. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	
XV	Se modificó y agregó contenido en el numeral: 15.1.2. Abordar la seguridad dentro de acuerdos con proveedores y Cadena de suministro de tecnología de información y comunicaciones.	
XVI	Se modificó y agregó contenido en el numeral: 16.1.3. Informes de debilidades de seguridad de información	