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, con excepción de los controles excluidos en la declaración de aplicabilidad.

II. FINALIDAD

Establecer los controles de Seguridad de la Información de la Norma ISO/IEC 27001 aplicables en la Zona Registral N° IX.

III. ALCANCE

El presente manual es de obligatorio cumplimiento para todo el personal que desarrolla actividades en las diversas unidades de organización de la Zona Registral N° IX, bajo cualquier modalidad de contrato.

IV. BASE LEGAL

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

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

4.2. Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal, publicado el 17 de julio de 2000.

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

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

4.5. 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, publicado el 14 de enero de 2016 y su modificatoria.

4.6. 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”, aprobada el 17 de julio de 2008 y sus modificatorias.

4.7. 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, aprobada el 18 de mayo de 2012 y su modificatoria.

4.8. Resolución de la Gerencia General de la Superintendencia Nacional de los Registros Públicos N° 077-2023-SUNARP/GG, que aprueba la Directiva DI 001-OTI, denominada: ¨Directiva para el Acceso a la Plataforma de TICs¨, aprobada el 29 de mayo de 2023.

V. TÉRMINOS Y DEFINICIONES

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

5.1. **Activo de información:** Es cualquier información que tenga valor para la organización o aquel recurso o sistema que lo contenga o realice el tratamiento de la misma.

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

5.3. **Copia No Controlada*:*** Es el documento copia del original sobre el cual no existe control de actualización. Si este documento Copia No Controlada no ha sido obtenido del repositorio pertinente poco antes de su uso, podría estar obsoleto. El uso de un documento obsoleto será responsabilidad del usuario, por lo tanto, debe verificar su vigencia en el repositorio o catálogo correspondiente.

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

5.5. **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.

5.6. **Incidente de seguridad de la información:** Evento único 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.

5.7. **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.).

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

5.9. **Mesa de Ayuda:** Es un servicio que ofrece información y soporte técnico a los usuarios de la Sunarp. Su propósito es atender solicitudes e incidentes internos y externos relacionados a la Plataforma de TICs.

5.10. **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.

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

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

5.13. Unidad de Organización*:* Es la denominación general que se emplea para referirse, según corresponda, a los órganos, unidades orgánicas, subunidades orgánicas y áreas que se formalizan en la estructura orgánica de la entidad, según su nivel organizacional*.*

5.14. Usuario: Persona registrada y debidamente autorizada a utilizar determinados recursos y servicios de la Plataforma de Tecnologías de la Información y Comunicación (TICs) con el fin de desarrollar actividades lícitas y se someten al cumplimiento de la normativa vigente.

- Se considera usuarios internos a los servidores civiles y practicantes.
- Se considera usuarios externos a proveedores de servicios y personal de terceros (contratistas y entidades con convenio) quienes se someten al estricto cumplimiento de su contrato laboral o de servicios, o al marco del convenio Institucional vigente, según corresponda.
- Se considera visitantes a usuarios debidamente autorizados por el personal directivo de la Sunarp.

VI. CONTROLES ORGANIZATIVOS

6.1. Políticas para la seguridad de la información [ISO 27001 A.5.1]

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 y están plasmadas en el documento “Política del Sistema Integrado de Gestión”, “Manual del Sistema Integrado de Gestión”, la “Directiva para el Acceso a la Plataforma de TICs” 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.

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.

6.2. Roles y responsabilidades para la seguridad de la información [ISO 27001 A.5.2]

a) La Zona Registral N° IX 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, según se indica en el “Manual del Sistema Integrado de Gestión”.

b) El Jefe de la Zona Registral N° IX 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.
c) Las funciones y responsabilidades del personal de la Zona Registral N° IX 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 de la Zona Registral N° IX" y en los procedimientos específicos.

6.3. Segregación de Funciones [ISO 27001 A.5.3]

a) Los propietarios de los activos de información deben autorizar el acceso teniendo en consideración una adecuada definición y segregación de funciones, de acuerdo con 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 de la Zona Registral N° IX" 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.

6.4. Responsabilidades de la Dirección [ISO 27001 A.5.4]

Todo personal que preste servicios en la Sunarp deberá cumplir con lo dispuesto en el numeral "V. RESPONSABILIDADES" de la "Directiva para el Acceso a la Plataforma de TICs".

Los servidores que ingresen a la Zona Registral N° IX 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.

6.5. Contacto con las autoridades [ISO 27001 A.5.5]

La Zona Registral N° IX cuenta con una lista de los principales teléfonos de emergencia, como son los de la policía, bomberos, emergencias médicas y defensa civil, los cuales se encuentran en carteles pegados en las diversas oficinas de la entidad y que deben ser usado por todos los servidores civiles y público en general ante los mencionados casos de emergencia. Sin embargo, en caso que la sede cuente con servicio médico funcionando en el momento del incidente o personal de seguridad se debe acudir con ellos en primer lugar en caso de ocurrir algún incidente correspondiente.

Para los casos específicos de incidentes de seguridad de la información o incidentes tecnológicos, los servidores civiles y proveedores deben contactar en primer lugar con la Mesa de Ayuda quienes deben atender o derivar el evento o incidente de seguridad de la información al especialista correspondiente.

Se tiene registrado en el formato “Lista de Contacto con Grupos de Interés Especial del Sistema de Gestión de Seguridad de la Información” una lista de autoridades en general, autoridades en seguridad de la información, proveedores que dan soporte a los diferentes activos de la información y contactos de la Sede Central, como el Oficial de Seguridad Digital.

6.6. Contacto con grupos de interés especial [ISO 27001 A.5.6]

a) El Oficial SGSI de la Zona Registral N° IX debe registrarse en foros que envíen actualizaciones respecto a seguridad de información y debe mantener constante relación con grupos de interés especial 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) Los contactos de los grupos de interés especial y de los foros deben estar registrados 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.

6.7. Inteligencia sobre Amenazas [ISO 27001 A.5.7]

Se debe recolectar y analizar las amenazas que podría afectar los activos de información de la organización, y establecer medidas de inteligencia para prevenirlas. De manera mensual y bajo demanda, el oficial de seguridad de la información debe llenar el formato de Recolección y Análisis de Amenazas, en dicho formato se establecerá la metodología a usar para el análisis de las amenazas, que incluye el establecimiento de controles y seguimiento.

Nota N° 01: En caso la amenaza identificada pueda afectar la confidencialidad, integridad y disponibilidad de la información en la organización, se procederá a establecer controles y realizar el análisis establecido en el formato Recolección y análisis de amenazas

Nota N° 02: En caso el análisis de inteligencia de amenazas resulte NO ACEPTABLE, esta información deberá ser gestionada en la matriz de riesgo del área, también podría haber ciertas amenazas como ACEPTABLES ser consideradas como riesgos dependiendo del criterio del oficial de seguridad de la información.

6.8. Seguridad de la información en la gestión de proyectos [ISO 27001 A.5.8]

La seguridad de la información debe estar integrada en la gestión de proyectos en cualquier tipo de proyecto.

Los proyectos de desarrollo de sistemas informáticos registrales y el de gestión documental son realizados por la Sede Central, por lo cual es la Sede Central quién gestiona los riesgos relacionados a esos proyectos.

Los otros proyectos desarrollados por la Zona Registral están ligados a las contrataciones de bienes o servicios, para lo cual las diferentes áreas

usuarias deben generar Especificaciones Técnicas o Términos de Referencia.

Es obligatorio que en las Especificaciones Técnicas y Términos de Referencia se deben incluir los siguientes controles para salvaguardar la seguridad de la información: cláusula de confidencialidad, cláusula de derechos de propiedad intelectual, el requerimiento de accesos a los sistemas o plataformas informáticas (si no está especificado no se le da acceso a ningún sistema). Además, es responsabilidad de las áreas usuarias especificar los controles que consideren necesarios incluir para la contratación para salvaguardar la seguridad de la información de la misma.

Para el caso de Términos de Referencia de más de 8 UIT, Especificaciones Técnicas que tengan una o más actividades de servicio como una implementación o configuración o una contratación de menos de 8 UIT en la cual el área usuaria considere necesario gestionar riesgos, se debe usar el formato “Plan de Gestión de Proyectos” en el cual el proveedor debe plasmar los riesgos a la seguridad de la información y proponer controles.

Una vez realizada la contratación, el área usuaria debe nombrar un personal del área que funcione como supervisor o responsable del proyecto. Esta persona debe hacer seguimiento a los controles establecidos para salvaguardar la seguridad de la información. En la reunión de inicio o Kick off debe establecerse conjuntamente con el proveedor los riesgos a la seguridad de la información existentes en el proyecto y los controles. De ocurrir un evento o incidente de seguridad de la información durante el desarrollo del proyecto, el responsable debe establecer controles y hacerles seguimiento.

6.9. Inventario de información y otros activos asociados [ISO 27001 A.5.9]

a) Se deberá cumplir con lo dispuesto en la “Directiva para el Acceso a la Plataforma de TICs” respecto al Inventario de Activos de Información, así como el instructivo que forma parte del formato “Inventario de Activos”.
b) La Zona Registral N° IX 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 los formatos: “Inventario de Activos”, “Inventario de Licencias de Software” y “Listado de Programas de la Sunarp”.
c) Para el desarrollo del Inventario de Activos de Información se debe realizar lo especificado en el instructivo que forma parte del formato “Inventario de Activos”.
d) 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.
e) El propietario del activo de información debe registrar el Inventario de Activos de Información en el formato “Inventario de Activos”.
f) Los jefes de cada unidad de organización con la finalidad de descentralizar y mejorar la eficiencia en la administración de la seguridad de información pueden delegar la propiedad de los activos de información a un servidor civil.

6.10. Uso aceptable de la información y otros activos asociados [ISO 27001 A.5.10]

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.
b) Los activos de información deben ser utilizados adecuadamente cualquiera sea el medio que los soporte y el ambiente en que se procesen.
c) Todo personal deberá cumplir con lo dispuesto en “Uso Aceptable de Activos de Información” que se encuentra dentro de la “Directiva para el Acceso a la Plataforma de TICs”.
d) 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.
e) 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.
f) 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.
g) Los documentos clasificados como confidenciales deben estar protegidos contra pérdida o robo.
h) Servidor civil es responsable de recoger inmediatamente los documentos que imprima en las impresoras asignadas, a fin de mantener la reserva de la información.
i) Las fotocopiadoras, escáneres o cualquier forma de tecnología de reproducción de la entidad deben ser utilizadas solo y exclusivamente por personas autorizadas.
j) Es responsabilidad de cada unidad de organización el destruir las impresiones que ya no sirven y que contienen información confidencial usando algún mecanismo de eliminación segura de información.
k) 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.

6.11. Devolución de activos [ISO 27001 A.5.11]

a) Al término o cambio de las responsabilidades de empleo se deberá cumplir con lo dispuesto en “Devolución de Activos de Información” que se encuentran dentro de la “Directiva para el Acceso a la Plataforma de TICs.”
b) La finalización del empleo debe incluir el retorno previo de los activos de información proporcionados por la Zona Registral N° IX servidor civil o tercero (de ser el caso) para el desempeño de las funciones asignadas.
c) 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.

d) La entrega y retorno de activos deberá realizarse según lo indicado en el documento “Reglamento Interno de los Servidores Civiles (RIS) de la Superintendencia Nacional de los Registros Públicos”.

6.12. Clasificación de la información [ISO 27001 A.5.12]

a) La información se clasifica en Público, Uso Interno y Confidencial:
   - Público: Para los activos de información cuyo contenido no es sensible, es de acceso público y su divulgación no genera impacto en la Zona Registral N° IX.
   - Uso Interno: Para los activos de información cuyo contenido sólo debe ser de uso y divulgación para el personal interno de la Zona Registral N° IX y que solo podrán ser divulgados a terceras partes teniendo firmado un acuerdo de confidencialidad, siempre y cuando su divulgación no impacte a la Zona Registral N° IX.
   - Confidencial: Para los activos de información cuyo contenido no debe ser divulgado ni distribuido a personas que no sean autorizadas y cuya difusión puede generar un impacto importante en la Zona Registral N° IX entre ellas: Pérdida económica, sanción legal o pérdida de imagen.

b) Los propietarios de los activos de información deben ser responsables de la clasificación del activo. La clasificación se debe registrar en el Inventario de Activos de Información en el formato “Inventario de Activos”.

6.13. Etiquetado de la información [ISO 27001 A.5.13]

a) Teniendo en consideración los niveles de clasificación mencionados en el punto anterior, la Zona Registral N° IX 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 (como los gabinetes de servidores) 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”.

6.14. Transferencia de información [ISO 27001 A.5.14]

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

a) 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.

b) 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.
c) 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.
d) 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.
e) 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.
f) Todo personal deberá cumplir con lo dispuesto en “Seguridad en el uso del Correo electrónico” que se encuentra dentro de la “Directiva para el Acceso a la Plataforma de TICs”
g) Las credenciales del correo electrónico son personales e intransferibles, 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.
h) 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.
i) 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.
j) 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.
k) 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.

6.15. Control de acceso [ISO 27001 A.5.15]

Se tiene una política de control de acceso en el numeral 6.1 “Política de Control de Acceso a la Plataforma de TICs” de la “Directiva para el Acceso a la Plataforma de TICs”.

a) Todo personal deberá cumplir con lo dispuesto en “Gestión de Identidades y Accesos a la Plataforma de TICs”, “Política de Control de Acceso a la Plataforma de TICs”, “Seguridad en la Plataforma de TICs” y “De la forma de solicitar el acceso a la Plataforma de TICs” que se

encuentran dentro de la “Directiva para el Acceso a la Plataforma de TICs”.

b) Los perfiles de acceso deben considerar los servicios de red y conexiones a las redes a los que un servidor civil puede tener acceso.
c) Se debe considerar la verificación de los medios usados para el acceso a los servicios de red.
d) 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 o de la infraestructura de escritorio virtual (VDI) y el perfil de los servidores civiles deben mantenerse durante las conexiones remotas a determinado sistema o servicio.
e) Las actividades asociadas a la alta, baja y modificación de usuarios para su acceso a la red de datos y 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”. Y las solicitudes para alta, baja y modificación de usuarios se deben realizar según lo establecido en el “Procedimiento Atención de Servicio de Mesa de Ayuda y Soporte a Usuarios”.
f) En ninguna circunstancia debe manipularse el contenido de un determinado directorio o carpeta de archivos 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 o carpetas de archivos 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.

6.16. Gestión de la identidad [ISO 27001 A.5.16]

a) Todo personal deberá cumplir con lo dispuesto en “Gestión de Identidades y Accesos a la Plataforma de TICs”, “Política de Control de Acceso a la Plataforma de TICs”, “Seguridad en la Plataforma de TICs” y “De la forma de solicitar el acceso a la Plataforma de TICs” que se encuentran dentro de la “Directiva para el Acceso a la Plataforma de TICs”.
b) 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”.
c) Las solicitudes para alta, baja y modificación de usuarios se deben realizar según lo establecido en el “Procedimiento Atención de Servicio de Mesa de Ayuda y Soporte a Usuarios”.
d) En caso de deshabilite o inactive 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 desactivados o bloqueados según lo indicado 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".

f) Es responsabilidad de la unidad de organización "Comunicar a la UTI, a través de la Mesa de Ayuda, el cese temporal o definitivo, así como la rotación promoción, encargo, destaque, traslado u otros de cada servidor civil en un plazo no mayor de un (01) día hábil de ocurrido, para la revocación de las credenciales de acceso la Plataforma de TICs a fin de evitar incidentes de seguridad de la información", según lo indicado en el 5.1.d) de la "Directiva para el acceso a la plataforma de TICs".

g) Es responsabilidad de la URH: "Comunicar a la UTI, a través de la Mesa de Ayuda, el cese temporal o definitivo, así como la rotación promoción encargo destaque traslado u otros de cada servidor/a civil en un plazo no mayor de un (01) día hábil de ocurrido, para la revocación de las credenciales de acceso la Plataforma de TICs" según lo indicado en el 5.4 de la "Directiva para el acceso a la plataforma de TICs".

6.17. Información de autentificación [ISO 27001 A.5.17]

a) Cada usuario de los sistemas de información de Zona Registral N° IX 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.

a) Todo personal deberá cumplir con lo dispuesto en "Información para la Autenticación de Usuarios" y "Responsabilidades de los Usuarios" que se encuentran dentro de la "Directiva para el Acceso a la Plataforma de TICs".

b) La contraseña de los usuarios para el acceso a los sistemas informáticos, plataformas y sistemas de red debe tener las siguientes características:
   - Secreta y no compartida.
   - Longitud mínima de 8 caracteres y máxima de 32 y deberá estar conformada por letras mayúsculas, minúsculas, números y caracteres especiales alfanuméricos.
   - Las cuentas de red deberán de quedar bloqueadas luego del tercer intento errado de una contraseña.
   - Las contraseñas de red deben ser forzadas a cambiarse periódicamente cada 45 días.
   - Las contraseñas temporales deben ser cambiadas inmediatamente por los usuarios una vez recibidas y verificadas. Esta acción es de responsabilidad del usuario. 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.

- No se deben incluir las contraseñas en ningún mecanismo automático de conexión que las deje almacenadas en el equipo.

c) 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".

6.18. Derecho de Acceso [ISO 27001 A.5.18]

a) Todo personal deberá cumplir con lo dispuesto en "Gestión de Identidades y Accesos a la Plataforma de TICs", "Política de Control de Acceso a la Plataforma de TICs", "Seguridad en la Plataforma de TICs" y "De la forma de solicitar el acceso a la Plataforma de TICs" que se encuentran dentro de la "Directiva para el Acceso a la Plataforma de TICs".

b) Cada usuario de los sistemas de información de Zona Registral N° IX 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) Las solicitudes para alta, baja y modificación de usuarios se deben realizar según lo establecido en el "Procedimiento Atención de Servicio de Mesa de Ayuda y Soporte a Usuarios".

e) En caso de deshabilite o inactive un identificador de usuario, no se debe volver a asignar a otra persona en el futuro.

f) En los casos de ceses, vacaciones, licencias de los trabajadores, los permisos y accesos a los sistemas de información deben ser desactivados o bloqueados según lo indicado 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".

g) Es responsabilidad de la unidad de organización "Comunicar a la UTI, a través de la Mesa de Ayuda, el cese temporal o definitivo, así como la rotación promoción, encargo, destaque, traslado u otros de cada servidor civil en un plazo no mayor de un (01) día hábil de ocurrido, para la revocación de las credenciales de acceso la Plataforma de TICs a fin de evitar incidentes de seguridad de la información", según lo indicado en el 5.1.d) de la "Directiva para el acceso a la plataforma de TICs".

h) Es responsabilidad de la URH: "Comunicar a la UTI, a través de la Mesa de Ayuda, el cese temporal o definitivo, así como la rotación promoción encargo destaque traslado u otros de cada servidor/a civil en un plazo no mayor de un (01) día hábil de ocurrido, para la revocación de las credenciales de acceso la Plataforma de TICs" según lo indicado en el 5.4 de la "Directiva para el acceso a la plataforma de TICs".

i) Según lo indicado en la "Directiva para el Acceso a la Plataforma de TICs", en la 7.1.1.e), la UTI deberá coordinar con la URH y comunicar a las unidades de organización los usuarios activos que tienen acceso a la Plataforma de TICs con sus respectivas autorizaciones vigentes, a fin de que sean depurados los que no correspondan. Dichas revisiones y coordinaciones se deberán efectuar con una periodicidad mínima de tres (03) meses.

Las unidades de organización deberán proporcionar la información que les sea solicitada para dicho fin.

j) Así mismo, el Oficial del SGSI de la Zona Registral N° IX revisará periódicamente los derechos de acceso, revocando los que hayan caducado o ya no correspondan con la función desempeñada por cada servidor civil.

6.19. Seguridad de la información en las relaciones con los proveedores [ISO 27001 A.5.19]

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

- Los términos de referencia y especificaciones técnicas de los proveedores deben contener cláusulas / acuerdos de confidencialidad en sus contratos, previa evaluación de su pertinencia por el área usuaria. Dichas cláusulas / acuerdos deberán comprometerlos a no divulgar, usar o explotar la información de la organización a la cual tengan acceso.

  A tal efecto en el Anexo N°1 se indica el modelo de la cláusula de confidencialidad.

- 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.

6.20. Abordar la seguridad de la información en los acuerdos con proveedores [ISO 27001 A.5.20]

a) Las unidades de organización que requieren los bienes o servicios de terceros deben definir en los términos de referencia o las especificaciones técnicas 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) En el caso que los proveedores requieran accesos a las plataformas informáticas, las unidades de organización deberán incluir, en los términos de referencia o las especificaciones técnicas, en "Recursos proporcionados por la Entidad", los recursos que se requieran como Correo electrónico para la comunicación y asignación del servicio a realizar, usuarios y accesos a los aplicativos (varios), accesos a páginas web de corresponder, equipos de cómputo y medios para la correcta ejecución del servicio. Una vez iniciado el servicio, el jefe de cada unidad de organización debe solicitar a la UTI, siguiendo lo establecido en el "Procedimiento Atención de Servicio de Mesa de Ayuda y Soporte a Usuarios". la asignación de accesos para las labores del tercero, adjuntando los términos de referencia o especificaciones técnicas donde se especifica los recursos a proporcionar La UTI creará los accesos, previa evaluación y disponibilidad de los recursos y accesos solicitados, 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".

6.21. Gestión de la seguridad de la información en la cadena de suministro de las TIC [ISO 27001 A.5.21]

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.

6.22. Seguimiento, revisión y gestión de cambios de los servicios de proveedores [ISO 27001 A.5.22]

a) Los servicios de terceros se deben monitorear y revisar de acuerdo con lo especificado en los términos de referencia o especificaciones técnicas, en la orden de servicio y/o en el contrato.
b) Se debe monitorear y revisar los registros y reportes emitidos por los servicios de terceros, para verificar el cumplimiento de los parámetros de seguridad de información establecidos. El monitoreo se realiza durante el periodo contratado del servicio y según actividades programadas.
c) Los jefes y personal de las unidades de organización deben comunicar las fallas e incidentes de seguridad de la información en los servicios de terceros a la Mesa de Ayuda.
d) Se deberá mantener la operación de la Zona Registral N° IX controlando el impacto de los servicios de terceros ante cambios regulados por la normatividad de contrataciones.
e) Se deben registrar todos los cambios y mejoras realizadas en los sistemas de comunicaciones u operaciones por servicios externos según la normatividad de contrataciones.
f) Se debe realizar la reevaluación de riesgos ante los cambios originados por las actividades del proveedor según lo precisado en el "Procedimiento para la Gestión de Riesgos de la Zona Registral N° IX".

6.23. Seguridad de la información para el uso de servicios en la nube [ISO 27001 A.5.23]

a) La Sede Central es responsable de la gestión del proceso de contratación del servicio en la nube establecido por la organización.
b) La Unidad de Tecnologías de la Información debe coordinar todos los requisitos de seguridad de la información pertinentes asociados con el uso de los servicios en la nube, así mismo los criterios de selección del servicio en la nube y alcance del uso del servicio en la nube.
c) La Unidad de Tecnologías de la Información debe hacer uso de las herramientas de control que la sede central haya delegado para la gestión del servicio en la nube.
d) En caso se produzcan incidentes en el uso de la nube estas serán gestionadas conforme al procedimiento de incidentes de seguridad vigente en la organización.
e) Los accesos al servicio de la nube serán gestionados conforme a lo establecido en las políticas de acceso vigente en la organización.
f) La Unidad de Tecnologías de la Información debe coordinar con la Sede Central que la información en la nube se elimine en caso culmine el contrato o cambie el proveedor o plataforma.

6.24. Planificación y preparación de la gestión de incidentes de seguridad de la información [ISO 27001 A.5.24]

a) La Zona Registral N° IX 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 la 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.

6.25. Evaluación y decisión sobre eventos de seguridad de la información [ISO 27001 A.5.25]

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 la Información”.

6.26. Respuesta a los incidentes de seguridad de la información [ISO 27001 A.5.26]

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 la 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.

6.27. Aprender de los incidentes de seguridad de la información [ISO 27001 A.5.27]

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 la Información”.

6.28. Recogida de pruebas [ISO 27001 A.5.28]

Frente a un incidente en la seguridad de la información, que involucre una acción disciplinaria o legal, la evidencia debe ser recolectada, mantenida y preservada por las áreas correspondientes.

La evidencia debe contar con características de autenticidad, confiabilidad, completitud y legalidad.

Cuando se trate de una evidencia digital, la Unidad de Tecnologías de la Información debe tomar las medidas necesarias para proteger la información digital; de manera que esta pueda ser confiable e integra.

Las denuncias relacionadas a la seguridad de la información serán tramitadas de acuerdo al “Procedimiento para la atención de comunicaciones y denuncias de presuntos actos de corrupción para la Zona Registral N° IX”.

Durante el procedimiento disciplinario, el jefe inmediato debe tomar las medidas necesarias con la finalidad de salvaguardar las evidencias que involucran a la información desviada, corresponde:

- Aislar, de ser posible, los equipos informáticos que pudieran servir de evidencia.

- Desconectar el equipo de la red de datos, para que ningún servidor pueda tener acceso a ella.
- En caso de equipos que se conectan a la red inalámbrica, como las computadoras portátiles; inhabilitar su acceso a dicha red.
- Solicitar la preservación de imágenes relacionadas al incidente dentro de los 30 días hábiles siguientes, resguardando los derechos de los titulares de los datos personales.

6.29. Seguridad de la información durante la interrupción [ISO 27001 A.5.29]

La Zona Registral N° IX 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 existe 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 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.

a) La Zona Registral N° IX 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”.
c) 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.
d) 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”.

6.30. Preparación de las TIC para la continuidad de la actividad [ISO 27001 A.5.30]

La Zona Registral N° IX cuenta con un Plan de Continuidad del Negocio, el cual tiene como alcance la aplicación de estrategias de continuidad basada en respaldo de la infraestructura de red, para ello tiene un centro de cómputo secundario redundante.

Se cuenta con un Análisis de Impacto al Negocio (BIA), se han definido estrategias de continuidad para afrontar escenarios de riesgos disruptivos, toda esta información y actividades se encuentra definido en el plan de continuidad de negocio.

6.31. Requisitos legales, reglamentarios y contractuales [ISO 27001 A.5.31]

Se debe identificar, documentar y mantener actualizados todos los requisitos legales, regulatorios y contractuales vigentes que pueden afectar a la seguridad de la información de la Zona Registral N° IX.

La identificación y documentación se realizará en el Intranet Institucional, en la siguiente ubicación: Sistemas de Gestión; Zona Registral N° IX; Documentos Internos y Externos; Áreas de Proceso de Gestión; Coordinación General del SIG.

El mantenimiento se realizará verificando las normas legales publicadas en el diario oficial peruano y en las alertas registrales (que informan las nuevas normas que afectan las actividades registrales). Ambas son enviadas diariamente por correo electrónico a todos los servidores civiles. Se actualizará en el Intranet.

6.32. Derechos de propiedad intelectual [ISO 27001 A.5.32]

Para proteger los derechos de propiedad intelectual se debe realizar lo siguiente:

La Unidad de Tecnologías de la Información (UTI) 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. El no cumplimiento de este control puede traducirse en la utilización de software adquirido en forma ilegal que comprometa la imagen y perjudicar económica o legalmente a la organización.

La UTI debe 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.

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

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

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.

La UTI deberá revisar 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.

Las Unidades de Organización deben contemplar aspectos referidos a los derechos de propiedad intelectual en las Especificaciones Técnicas y los Términos de Referencia que preparen.

6.33. Protección de los registros [ISO 27001 A.5.33]

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 de organización 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", y de los registros electrónicos es la UTI, según el caso, quienes en coordinación con los responsables de las unidades de organización 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 de organización 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 datos de información que se encuentran bajo su custodia.

6.34. Privacidad y protección de la información personal [ISO 27001 A.5.34]

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 las Resoluciones Directorales emitidas 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 "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.

6.35. Revisión independiente de la seguridad de la información [ISO 27001 A.5.35]

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 SIG 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".

6.36. Cumplimiento de las políticas, reglas y normas de seguridad de la información [ISO 27001 A.5.36]

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 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.
d) Todos los sistemas informáticos de la Zona Registral N° IX 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.

6.37. Procedimientos operativos documentados [ISO 27001 A.5.37]

a) Se debe identificar qué actividades del trabajo deben ser documentadas 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 con los procesos que se realizan en la Zona Registral N° IX y deberán seguir las actividades y lineamientos definidos en el "Procedimiento de Gestión de Documentos de Soporte a los Procesos".

VII. CONTROLES DE PERSONAS

7.1. Selección [ISO 27001 A.6.1]

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 servidores civiles de la Zona Registral N° IX, la URH debe seguir los lineamientos establecidos en el Reglamento Interno de los Servidores Civiles de la Superintendencia Nacional de los Registros Públicos -Sunarp.
- Para la evaluación del personal encargado de las labores registrales se debe seguir lo establecido en el Reglamento de Acceso a la Función Registral dentro del Sistema Nacional de los Registros Públicos.
- 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.

7.2. Condiciones de empleo [ISO 27001 A.6.2]

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.

7.3. Sensibilización, educación y formación en materia de seguridad de la información [ISO 27001 A.6.3]

a) Se debe desarrollar charlas de concientización y sensibilización a los servidores de la Zona Registral N° IX, 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 los jefes de unidades de organización deben facilitar o asegurar que su personal asista.

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.

7.4. Proceso disciplinario [ISO 27001 A.6.4]

En el caso que el servidor civil incumpla alguna regulación establecida por el Sistema de Gestión de Seguridad de la Información, de acuerdo al artículo 95 literal x) del RIS esto sería considerado como una falta a las obligaciones del servidor y por lo tanto según el artículo 101 literal e) sería considerado como falta leve y por lo tanto pasible de sanción administrativa disciplinaria.

El procedimiento administrativo disciplinario se rige por lo dispuesto en la Ley N° 30057, Ley del Servicio Civil, en el Título V, Capítulo II y en el Reglamento de la mencionada Ley, Título VI, y demás normas reglamentarias emitidas por la Autoridad del Servicio Civil - SERVIR.

7.5. Responsabilidades tras el cese o el cambio de empleo [ISO 27001 A.6.5]

a) Al término o cambio de las responsabilidades de empleo se deberá cumplir con lo dispuesto en “Gestión de Identidades: Baja o suspensión de accesos” y “Devolución de Activos de Información” que se encuentran dentro de la “Directiva para el Acceso a la Plataforma de TICs.”
b) La URH debe informar oportunamente los ceses de los servidores a las Unidades Orgánicas respectivas de la Zona Registral N° IX que correspondan, para tomar las medidas preventivas y correctivas necesarias.
c) En cuanto al cambio de responsabilidades del empleo, es de responsabilidad de la unidad de organización informar oportunamente a la Unidad de Tecnologías de la Información - UTI sobre los perfiles y privilegios que se revocarán según lo indicado en el 5.1.d) de la “Directiva para el acceso a la plataforma de TICs”: Comunicar a la UTI, a través de la Mesa de Ayuda, el cese temporal o definitivo, así como la rotación promoción, encargo, destaque, traslado u otros de cada servidor civil en un plazo no mayor de un (01) día hábil de ocurrido, para la revocación de las credenciales de acceso la Plataforma de TICs a fin de evitar incidentes de seguridad de la información”
d) Es responsabilidad de la URH: “Comunicar a la UTI, a través de la Mesa de Ayuda, el cese temporal o definitivo, así como la rotación promoción encargo destaque traslado u otros de cada servidor/a civil en un plazo no mayor de un (01) día hábil de ocurrido, para la revocación de las credenciales de acceso la Plataforma de TICs” según lo indicado en el 5.4 de la “Directiva para el acceso a la plataforma de TICs”.
e) Al término del empleo el servidor se encuentra obligado a presentar la entrega de cargo dispuesto en el Reglamento Interno de Servidores Civiles (RISC), en el mismo se comprende el reporte de no adeudos de documentos, bienes y/o fondos, en cuyo literal e) “La Oficina de Tecnologías de la Información o la que haga sus veces en los Órganos Desconcentrados, deja constancia que el/la servidor/a que entrega el

cargo, no adeuda ni tiene pendiente entrega de equipos informáticos y/o accesorios" que es aplicable a la Unidad de Tecnologías de la Información. Asimismo, dicha entrega de cargo comprende la "declaración jurada de no retirar documentación y compromiso de confidencialidad".

7.6. Acuerdos de confidencialidad o no divulgación [ISO 27001 A.6.6]

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 extenderse incluso hasta después del cese de la relación contractual o laboral con la organización.

7.7. Trabajo a distancia [ISO 27001 A.6.7]

Todo personal que preste servicios en la modalidad de teletrabajo deberá cumplir con lo dispuesto en "Teletrabajo o Trabajo remoto" que se encuentra dentro de la "Directiva para el Acceso a la Plataforma de TICs."

La Zona Registral N° IX también brinda servicios de conexiones externas mediante una infraestructura de escritorios virtuales (VDI) además de las conexiones de tipo VPN para los usuarios debidamente identificados, autorizados y autenticados con doble factor de autenticación.

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.

Para que el trabajador pueda trabajar en la modalidad de teletrabajo debe seguir los lineamientos establecidos en la Ley 31572 (Ley del Teletrabajo), el Reglamento del Teletrabajo (D.S. 2-2023-TR), el Plan de Teletrabajo en la Sunarp, la Lista de Puestos Teletrabajables y toda otra normativa relacionada.

7.8. Informes de eventos de seguridad de la información [ISO 27001 A.6.8]

Cualquier servidor civil debe reportar incidentes o eventos detectados o sospechas que se tengan, según los lineamientos definidos en el documento "Procedimiento de Gestión de Incidentes de Seguridad de la 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".

- 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.

VIII. CONTROLES FISICOS

8.1. Perímetro de seguridad física [ISO 27001 A.7.1]

a) La Zona Registral N° IX debe asegurar que los entornos de almacenamiento de información cuenten con un perímetro físico que brinde un nivel de protección acorde con la clasificación de la información, aplicando el principio de proporcionalidad.
b) Deben establecerse controles de seguridad que regulen el ingreso, permanencia y salida del personal, contratistas, proveedores, público en general y bienes, asegurando su registro, monitoreo y validación.
c) Todos los servidores civiles, cualquiera sea su condición contractual, que desee ingresar a las oficinas de la Zona Registral N° IX, 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.
d) 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.
e) 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 visitante se hace responsable por las acciones inapropiadas que perjudiquen a la entidad, en el momento de ingreso, si el visitante niega que porta equipamiento tecnológico y posteriormente se identifica la presencia de dicho equipamiento, se procederá la comunicación de este hecho al área de Seguridad, para realizar la inmovilización, dada la advertencia al ingreso y se tomarán las acciones que resulten necesarias según la "Guía de actuación del personal de seguridad y vigilancia contra intrusión en la Zona Registral N° IX.
f) No se debe permitir el ingreso de personal interno y terceros, sin las autorizaciones correspondientes o que no sigan el procedimiento adecuado.
g) Los servidores civiles de la Zona Registral N° IX 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.

h) Los sistemas críticos que gestionen información confidencial deben ubicarse en entornos físicos restringidos, aislados de usuarios no autorizados, y contar con **controles de acceso físico[1], lógico[2] y ambiental[3]** que aseguren su protección integral, los cuales deben ser evaluados periódicamente.
i) En lo posible, las oficinas deben quedar cerradas cuando no hay personas en su interior.
j) 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.

8.2. Entrada física [ISO 27001 A.7.2]

a) Todos los servidores civiles, que ingresen a las oficinas de la Zona Registral N° IX, deberán portar el fotocheck, de manera permanente y visible a la altura del pecho, en todo momento que se encuentre dentro de la Entidad.

---

[1] **Un control físico** protege un espacio o equipamiento impidiendo físicamente que personas no autorizadas entren, accedan o manipulen la infraestructura. Son la primera línea de defensa en seguridad de la información.
Ejemplos de controles físicos:
– Puertas reforzadas y cerraduras de alta seguridad.
– Tarjetas de acceso, llaveros electrónicos o biometría (huella, rostro, iris).
– Guardias de seguridad en el perímetro o entradas.
– Circuito cerrado de televisión (CCTV) para monitorear accesos.
– Detectores de metales en zonas restringidas.
– Torniquetes o molinetes en accesos controlados.
– Barreras físicas como rejas, muros o cercas perimetrales.
– Custodia y registro de visitantes.

[2] **Un control lógico** limita o protege el acceso a la información usando tecnología, no usando barreras físicas como puertas o cerraduras. Ejemplos de controles lógicos serían:
– Contraseñas seguras (para entrar a un sistema o computadora).
– Autenticación multifactor (como pedir además un código del celular).
– Roles y perfiles de acceso (que cada usuario solo pueda ver o modificar lo que le corresponde).
– Encriptación de información (para que, aunque alguien robe datos, no pueda leerlos).
– Firewalls o cortafuegos (que bloquean accesos no autorizados).
– Software antivirus o antimalware.

[3]**Un control ambiental** protege los equipos y la información frente a riesgos naturales o del entorno físico, como el calor, el agua, el fuego o la falta de electricidad. Ejemplos de controles ambientales serían:
– Sistemas de detección y extinción de incendios (detectores de humo, rociadores automáticos).
– Protección contra sobretensiones eléctricas (UPS, estabilizadores).
– Sistemas de climatización adecuados (aire acondicionado para evitar sobrecalentamiento de servidores).
– Sensores de humedad o inundación.
– Alarma de gases o escapes tóxicos (en salas de servidores).
– Puertas cortafuego y sellado de áreas críticas.
– Generadores eléctricos de respaldo (en caso de corte de energía).

b) 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.
c) 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 visitante se hace responsable por las acciones inapropiadas que perjudiquen a la entidad, en el momento de ingreso, si el visitante niega que porta equipamiento tecnológico y posteriormente se identifica la presencia de dicho equipamiento, se procederá la comunicación de este hecho al área de Seguridad, para realizar la inmovilización, dada la advertencia al ingreso y se tomarán las acciones que resulten necesarias según la "Guía de actuación del personal de seguridad y vigilancia contra intrusión en la Zona Registral N° IX ".
d) No se debe permitir el ingreso de personal interno y terceros, sin las autorizaciones correspondientes o que no sigan el procedimiento adecuado.
e) Los servidores civiles de la Zona Registral N° IX 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.

8.3. Asegurar las oficinas, salas e instalaciones [ISO 27001 A.7.3]

a) Los sistemas críticos que manejen información de la Zona Registral N° IX deben estar en entornos restringidos, aislados de los usuarios comunes y deben tener controles de acceso físico y lógico seguros.
b) En lo posible, las oficinas deben quedar cerradas cuando no hay personas en su interior.
c) 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.
d) El personal debe verificar que ventanas, puertas, archivadores y otros medios de almacenamiento de información estén debidamente cerrados al momento de su retiro, como parte de las medidas de protección del entorno físico.

8.4. Vigilancia de la seguridad física [ISO 27001 A.7.4]

a) La Zona Registral N° IX dispone de un servicio de vigilancia para asegurar el perímetro, oficinas y demás ambientes ante intrusiones físicas.

b) Se tiene implementado cámaras de video vigilancia, algunas con ellas con sensores de movimientos, así como sensores de humo en los ambientes y en lugares de alto tránsito.
c) Controles biométricos para el acceso a los Centros de Datos.
d) Se tiene establecido varios niveles de vigilancia física, incluso el personal de seguridad realiza rondas con cierta frecuencia por los ambientes de la organización.

8.5. Protección contra las amenazas físicas y medioambientales [ISO 27001 A.7.5]

a) Las unidades de organización deben contar con protección física contra amenazas ambientales, desastres naturales, ataques maliciosos, disturbios civiles o accidentes.
b) La Zona Registral N° IX 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, sensores de temperatura, sensores 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.

8.6. Trabajar en zonas seguras [ISO 27001 A.7.6]

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 de detectores de humo. El jefe de la unidad de organización deberá verificar el cumplimiento del presente ítem.
b) No se debe proveer información sobre la ubicación de los Gabinetes de Comunicaciones 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 de organización respectivas y supervisadas continuamente.
d) 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.
e) 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 de organización respectiva debe autorizar, supervisar y comunicar dicho acceso al agente de seguridad de turno.

8.7. Escritorio y pantalla despejados [ISO 27001 A.7.7]

Todo personal deberá cumplir con lo dispuesto en “Política de Puesto de trabajo despejado y bloqueo de pantalla” que se encuentra dentro de la “Directiva para el Acceso a la Plataforma de TICs”.

8.8. Ubicación y protección de los equipos [ISO 27001 A.7.8]

a) La Zona Registral N° IX 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 Centro de Datos deberá contar con un mecanismo de suministro eléctrico ininterrumpido (UPS), de manera que suministre electricidad de respaldo cuando se producen cortes o fluctuaciones de energía.
c) Se deben monitorear las condiciones ambientales como temperatura y humedad, que puedan afectar negativamente la operatividad de los equipos del Centro de Datos.
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 de organización 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.

8.9. Seguridad de los activos fuera de las instalaciones [ISO 27001 A.7.9]

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 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.

8.10. Medios de almacenamiento [ISO 27001 A.7.10]

a) Todo personal deberá cumplir con lo dispuesto en “Política de dispositivos móviles” y “Medios de almacenamiento” que se encuentran dentro de la “Directiva para el Acceso a la Plataforma de TICs”.

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

c) 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.

d) Según lo indicado en la "Directiva para el Acceso a la Plataforma de TICs", en el numeral 7.2.5: "considerando el uso de USB como el mayor vector de infección de malware, la Sunarp restringe el uso controlado de memorias de almacenamiento tipo USB. En casos muy excepcionales, la OTI/UTI apoyará en la grabación o recuperación de información contenida en los dispositivos USB/CD/DVD, debiendo seguir un protocolo de prevención que garantice estar libre de amenazas (por ejemplo, escaneo con antivirus u otras herramientas)".

   "El uso de medios extraíbles está restringido se permitirá excepcionalmente solo si es absolutamente necesario, "cuando no existe otra opción mejor".

e) En los casos excepcionales que se requiera la habilitación de los puertos USB para el uso de los medios removibles, como, por ejemplo, trasladar información para capacitación o eventos, deberán ser solicitados formalmente, indicando una justificación debidamente motivada, siguiendo los lineamientos definidos en el documento "Procedimiento de Atención de Servicio de Mesa de Ayuda y Soporte a Usuarios" e indicando el lapso de tiempo que durará la habilitación mencionada.

f) Así mismo los usuarios deben evitar el uso de programas no autorizados.

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.

a) Cualquier información confidencial que se encuentre en un medio físico y deba ser trasladada desde la Zona Registral N° IX 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) En el caso de que se requiera una transferencia segura de información digital a través de un medio removible, se realizará la encriptación del archivo. El método de encriptación a usar consistirá en que el emisor encriptará la información con una contraseña y se encargará de hacer llegar esa contraseña al receptor en forma reservada y confidencial, para que pueda desencriptar la información encriptada, en caso aplique, como, por ejemplo, cuando se transfiere información confidencial o que requiere conservar su

integridad a través de un medio removible o una red pública. La UTI evaluará el medio para la encriptación y gestionará su adquisición u obtención.

c) 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".

La Zona Registral N° IX 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".

8.11. Servicios públicos de apoyo [ISO 27001 A.7.11]

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.

8.12. Seguridad del cableado [ISO 27001 A.7.12]

a) La Zona Registral N° IX 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.

8.13. Mantenimiento de los equipos [ISO 27001 A.7.13]

a) El mantenimiento de equipos de cómputo 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 o el autorizado por dicha unidad 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.

8.14. Eliminación segura o reutilización de los equipos [ISO 27001 A.7.14]

Todos los equipos que son operados en la Zona Registral N° IX, 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.

IX. CONTROLES TECNOLOGICOS

9.1. Dispositivos de punto final del usuario [ISO 27001 A.8.1]

Todo personal que preste servicios en la Sunarp y tenga asignado un equipo móvil deberá cumplir con la "Política de Dispositivos Móviles" que se encuentra dentro de la "Directiva para el Acceso a la Plataforma de TICs."

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

9.2. Derechos de acceso privilegiados [ISO 27001 A.8.2]

Los usuarios administradores deberán cumplir con lo dispuesto en "Gestión de Acceso Privilegiado: Servidores alojados en centro de datos" y "Gestión de Acceso Privilegiado: Base de Datos" que se encuentran dentro de la "Directiva para el Acceso a la Plataforma de TICs".

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".

9.3. Restricción del acceso a la información [ISO 27001 A.8.3]

Todo personal deberá cumplir con lo dispuesto en "Política de Control de Acceso a la Plataforma de TICs" que se encuentra dentro de la "Directiva para el Acceso a la Plataforma de TICs".

Los servidores civiles tendrán derecho a acceder a la información según los permisos de usuario asignados. En la generación de permisos, se debe controlar los derechos de acceso a lectura, escritura, borrado y ejecución, según los documentos “Procedimiento Atención de Servicio de Mesa de Ayuda y Soporte a Usuarios” y “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. Acceso al código fuente [ISO 27001 A.8.4]

NO APLICA

9.5. Autenticación segura [ISO 27001 A.8.5]

f) 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.
g) 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.
h) Los servidores civiles deberán proteger el acceso a su máquina activando el protector de pantalla (con las teclas Windows + L) 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.
i) 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.
j) 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.

9.6. Gestión de la capacidad [ISO 27001 A.8.6]

La UTI de la Zona Registral N° IX 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 y se debe monitorear el uso de los recursos informáticos, según lo indicado en el “Procedimiento de gestión de la capacidad de los recursos informáticos”.

Con respecto a las capacidades a nivel de personas, la Sede Central gestiona directamente la cantidad de servidores civiles, pero teniendo en cuenta que las entidades públicas son gestionadas por medio de la asignación presupuestaria otorgado por el Ministerio de Economía, por ello, para el CAP aplica el Presupuesto Analítico de Personal (PAP) aprobado para el Año Fiscal y para el personal basado en el régimen de contratación CAS se tiene establecido la ley N° 32185 por el cual se gestiona la cantidad de personal anual para todas las actividades de la SUNARP.

9.7. Protección contra el malware [ISO 27001 A.8.7]

La Zona Registral N° IX 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, 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.
- En caso un servidor civil detecte código malicioso en un equipo, debe informar inmediatamente a Mesa de Ayuda para que aísle el equipo y tome las medidas necesarias.

9.8. Gestión de las vulnerabilidades técnicas [ISO 27001 A.8.8]

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.

9.9. Gestión de la configuración [ISO 27001 A.8.9]

La Zona Registral N° IX realiza actividades básicas de configuración en los equipos de seguridad perimetral y comunicaciones, los cuales están indicados en los "Lineamientos para las configuraciones de equipos de comunicaciones de red y seguridad". En algunos casos La Zona Registral N° IX coordina el proceso de configuración con la Sede Central.

9.10. Eliminación de información [ISO 27001 A.8.10]

a) La eliminación de la información digital / electrónica, se realiza mediante técnicas de formateo establecido en las herramientas que actualmente utiliza la organización
b) La eliminación de la información impresa, se realiza en la base al Procedimiento Administrativo del Archivo Central, es decir se elabora un expediente de eliminación se remite al Archivo General de la Nación para su aprobación y la documentación autorizada para su eliminación lo recoge el AGN.

9.11. Enmascaramiento de datos [ISO 27001 A.8.11]

NO APLICA, debido a que el desarrollo de los sistemas de información incluido la aplicación de alguna técnica de enmascaramiento de datos, se realizan en la Sede Central.

9.12. Prevención de la fuga de datos [ISO 27001 A.8.12]

La organización ha establecido una seria de medidas de prevención para prevenir la fuga de datos, las medidas son:

a) Prevención Correo Electrónico Institucional

La organización ha aplicado las siguientes políticas de correo institucional:

- El tamaño máximo de archivos adjuntos es de 20 MB
- Está restringido el envío de correos desde dominios externos al correo institucional. (Siempre y cuando no se tenga el correo externo como contacto registrado o conocido).
- Está restringido el compartido de archivos mediante Google Drive a dominios externos a la Entidad (Salvo excepciones con previa autorización).
- Bloqueo de dominios externos sospechosos o maliciosos (spam, phishing)
- Está restringido el envío de archivos con ciertas extensiones (exe, .dwg).

b) Prevención Uso de Puertos USB
- Se tiene configurado el control de dispositivos mediante la Consola de Antivirus, el cual bloquea puertos USB, CD/DVD, adaptadores wifi, bluetooth, etc.
- Según funcionalidad del equipo de cómputo, se procede con el bloqueo de puertos USB físicos a nivel de BIOS (Dicha actividad debe coordinarse con Mesa de Ayuda de la Zona Registral N° IX)..

c) Prevención Uso de Puertos de red
- Aplicación de seguridad de puertos en los switches de comunicaciones.

d) Prevención Uso WIFI
- Se ha configurado un “Identificador de Conjunto de Servicios - SSID” (nombre de la red inalámbrica) con autenticación por contraseña (previa habilitación de la MAC address del equipo) para las PC, tablets, teléfonos móviles.
- Se ha configurado un SSID con autenticación de dominio de red (usuario y clave de dominio) para las PC.

e) Otras medidas de prevención
- Se tiene habilitado el uso de BitLocker para la encriptación de data en los equipos portátiles (laptop) de la entidad.
- Políticas de acceso a internet (uso restringido de páginas web para transferencias de archivos).
- Los enlaces de datos funcionan como una red IP/VPN lo que establece un canal privado de la información exclusiva para la Entidad.
- Se tienen enlaces de fibra óptica dedicados para la Entidad para la transferencia de información entre los Centro de Datos.
- El acceso a unidades compartidas mediante políticas de unidad organizativa y grupo de dominio.

9.13. Información de respaldo [ISO 27001 A.8.13]

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” y “Procedimiento para la restauración de las copias de seguridad (backup)”.

9.14. Redundancia de las instalaciones de tratamiento de la información [ISO 27001 A.8.14]

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

9.15. Registro [ISO 27001 A.8.15]

a) Las aplicaciones de la Zona Registral N° IX 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 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.
c) La Zona Registral N° IX 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.
d) El Oficial del SGSI debe realizar supervisiones de manera periódica para revisar el cumplimiento de este control.
e) 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.
f) El Oficial del SGSI debe realizar supervisiones de manera periódica para revisar el cumplimiento de este control.

9.16. Actividades de seguimiento [ISO 27001 A.8.16]

La Zona Registral N° IX tiene al centro de operaciones de red (NOC) para realizar las siguientes actividades:

- Monitoreo 24/7 de los sistemas críticos del Centro de Datos Principal (CDP) y Centro de Datos Secundario (CDS) con sus respectivas Salas Eléctricas.
- Identificación y gestión de alertas generadas tanto por las herramientas de monitoreo como alertas físicas en los equipos.
- Creación y seguimiento de tickets.

- Coordinación con el personal de facilities para la atención de incidentes de primer nivel.
- Escalamiento de incidencias a niveles superiores según criticidad.
- Análisis de tendencias y generación de reportes de alertas.
- Adicional se realizan 2 recorridos presenciales en el día a los centros de datos, salas eléctricas y área de Dry Cooler, donde se verifica el estado y funcionamiento de equipos en general con su respectiva toma de parámetros, estado de piso, techo y limpieza de los ambientes.
- Reporte y registro en la plataforma de gestión de tickets, de los recorridos con el estado de los ambientes y los parámetros de medición encontrados mediante el formato de check list diario.
- Control del retiro de las láminas atrapa polvo según la frecuencia definida, ubicadas en la entrada de los centros de datos.
- Registro y control de bitácora de ingreso y salida de los centros de datos y bitácora de incidentes y requerimientos.

Las herramientas de monitoreo

El NOC emplea herramientas para la supervisión y gestión de los Centros de Datos, estas herramientas realizan las siguientes actividades:

- Monitoreo del grupo electrógeno, control de acceso, aires acondicionados, UPS, tablero estabilizado, tablero comercial, panel contra incendios y otros sistemas de infraestructura.
- Plataforma para la gestión de tickets y administración de activos.
- Supervisión del estado de servidores, almacenamiento (storage) y switches.
- Monitoreo avanzado de infraestructura crítica y energética.
- Monitoreo de temperaturas y humedad de los Centros de Datos y Salas Eléctricas.
- Por medio de la interfaz web se monitorea temperatura, humedad y aperturas de las puertas de los gabinetes.
- Por medio de la interfaz web se monitorea el funcionamiento de los aires acondicionados de precisión del CDP.

Alarmas Gestionadas

Las alarmas monitoreadas por el NOC se categorizan en tres áreas principales:

- Infraestructura física: Alarmas relacionadas con fallas en el suministro eléctrico, temperatura, humedad, alertas físicas en equipos y accesos no autorizados.

- Red y servidores: Alertas sobre caídas de servicios, picos de uso, latencia elevada y problemas de conectividad.
- Seguridad de la información: Detección de accesos no autorizados y posibles amenazas.

Procedimiento ante Incidencias de Seguridad de la Información Para garantizar la protección de la información y cumplir con los requisitos de ISO/IEC 27001:2022, el NOC cumple con el procedimiento ante incidentes de seguridad vigente en la organización.

9.17. Sincronización de relojes [ISO 27001 A.8.17]

Todos los relojes de los sistemas de procesamiento de información de la Zona Registral N° IX 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.

9.18. Uso de programas de utilidad privilegiados [ISO 27001 A.8.18]

En la Zona Registral N° IX 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.

9.19. Instalación de software en sistemas operativos [ISO 27001 A.8.19]

a) La Zona Registral N° IX 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”.
e) La UTI es la única Unidad Orgánica autorizada para realizar instalación de software en la Zona Registral N° IX.
f) Para todos los equipos de cómputo propiedad de la Zona Registral N° IX, se debe instalar únicamente el software que cuente con licencia

autorizada o software libre de uso autorizado para uso en la organización.

g) 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.

9.20. Seguridad de las redes [ISO 27001 A.8.20]

a) Todo personal deberá cumplir con lo dispuesto en “Política de Control de Acceso a la Plataforma de TICs”, “Seguridad en la Plataforma de TICs” y “Gestión de Identidades y Accesos a la Plataforma de TICs” que se encuentran dentro de la “Directiva para el Acceso a la Plataforma de TICs”.
b) 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.
c) 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.
d) 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 la Internet.

9.21. Seguridad de los servicios de red [ISO 27001 A.8.21]

a) Todo personal deberá cumplir con lo dispuesto en “Sobre el Uso de Internet” que se encuentra dentro de la “Directiva para el Acceso a la Plataforma de TICs”.
b) 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.
c) Los servicios de red deben contar con mecanismos de detección y eliminación de código malicioso.
d) Los accesos a la red internos y externos deben contar con mecanismos de seguridad perimetrales.

9.22. Segregación de redes [ISO 27001 A.8.22]

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.

9.23. Filtro web [ISO 27001 A.8.23]

En la organización se aplica las siguientes medidas de restricción de navegación web:

a) A través de un Proxy Web y Firewall perimetral que es administrado por la Sede Central.

b) Se bloquea el acceso a ciertos dominios o páginas web restringidos a través del Firewall perimetral de Zona IX.
c) Las políticas de navegación a internet son administradas por la Sede Central según la directiva de acceso a Internet.
d) Se cuenta con un control de bloqueo de IPs y dominios maliciosos a través del Firewall Perimetral que han sido identificados como indicadores de compromiso IoC.
e) La directiva de acceso a internet es actualizada por la Sede Central

9.24. Uso de la criptografía [ISO 27001 A.8.24]

a) La Zona Registral N° IX 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.

- En el caso de que se requiera una transferencia segura de información digital a través de un medio removible esto se realizará mediante la encriptación simétrica del archivo en la cual el emisor dará en forma confidencial una contraseña al responsable de la parte receptora. La UTI evaluará el medio para la encriptación y gestionará su adquisición u obtención.

b) Las claves de las encriptaciones realizadas a las copias de respaldo 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”.

9.25. Ciclo de vida de desarrollo seguro [ISO 27001 A.8.25]

Todos los sistemas de información registrales y administrativos a cargo de la Sede Central son diseñados, desarrollados y mantenidos por la Sede Central.

Sobre estos sistemas de información, las Zonas Registrales no pueden hacer desarrollos o mantenimientos.

La Zona Registral puede solicitar a la Sede Central que se realicen modificaciones a los sistemas registrales o los sistemas administrativos a cargo de la Sede Central. En esos casos, la Unidad Registral o la Unidad responsable de la ejecución del proceso, puede solicitar a la UTI que verifique la factibilidad técnica de lo solicitado. La UTI debe incorporar, en este informe de factibilidad técnica, los requerimientos de seguridad de la información que considere necesarios. Luego la Unidad Registral o la unidad responsable lo remite a la Sede Central, a través de Jefatura Zonal.

Se debe asegurar que al entorno de desarrollo tenga acceso solo las personas responsables y que esté protegido contra amenazas.

Se debe implementar un control de versiones para gestionar los cambios en el código de manera segura.

9.26. Requisitos de seguridad de las aplicaciones [ISO 27001 A.8.26]

Todos los sistemas informáticos registrales y administrativos que están a cargo de la Sede Central, son diseñados, desarrollados y mantenidos por la Sede Central. Estas actividades no pueden ser realizadas por las Zonas Registrales. Esto incluye tanto los aplicativos de uso interno, como los servicios de aplicaciones sobre redes públicas, como las transacciones de estos servicios de aplicación.

Los sistemas y aplicaciones informáticos utilizados por los procesos dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI) se encuentran identificados en el formato "Listado de Programas de la Sunarp".

Asimismo, se tienen en cuenta los siguientes aspectos:

a) La Unidad de Tecnologías de la Información, de acuerdo a su competencia, realizará el análisis de los sistemas existentes, incluyendo la seguridad de la información y propondrá a las unidades correspondientes la validación y ejecución del análisis presentado.

b) La Zona Registral puede solicitar a la Sede Central que se realicen modificaciones a los sistemas registrales o administrativos a cargo de la Sede Central. En esos casos, las unidades de organización remiten sus requerimientos de modificación a la Unidad Registral o Unidad responsable de la ejecución del proceso (si es administrativo), quien verifica la factibilidad de lo solicitado y consolida los requerimientos.

- De ser un cambio que la Unidad Registral o Unidad responsable de la ejecución del proceso (si es administrativo) considere que es simple y que no requiere la verificación técnica de la Unidad de Tecnologías de la Información (UTI) lo remite al Órgano competente de la Sede Central.
- En caso que el cambio no sea simple, como por ejemplo el requerimiento de una nueva funcionalidad o de un nuevo aplicativo, la Unidad Registral o Unidad responsable de la ejecución del proceso (si es administrativo) remite los requerimientos a la Unidad de Tecnologías de la Información (UTI) para que verifique la factibilidad técnica de lo solicitado. La UTI debe incorporar, en este informe de factibilidad técnica, los requerimientos de seguridad de la información que considere necesarios y remitirlo a la Unidad Registral o Unidad responsable de la ejecución del proceso (si es administrativo).

  Recibido este informe la Unidad Registral o Unidad responsable de la ejecución del proceso (si es administrativo) remite el requerimiento de modificación, considerando los requerimientos de seguridad de la información, al Órgano competente de la Sede Central.
- La Dirección Técnica Registral o el órgano competente analizará los requerimientos y de considerarlo válido los remitirá a la Oficina

de Tecnologías de la Información (OTI) de la Sede Central para su implementación, indicándole la prioridad que le debe dar a dicho desarrollo o mantenimiento.

9.27. Arquitectura de sistemas seguros y principios de ingeniería [ISO 27001 A.8.27]

NO APLICA,

debido a que el desarrollo de los sistemas de información incluidos en el alcance, se realizan en la Sede Central.

9.28. Codificación segura [ISO 27001 A.8.28]

NO APLICA,

debido a que el desarrollo de los sistemas de información incluidos en el alcance, se realizan en la Sede Central.

9.29. Pruebas de seguridad en el desarrollo y la aceptación [ISO 27001 A.8.29]

NO APLICA,

debido a que el desarrollo de los sistemas de información incluidos en el alcance, se realizan en la Sede Central.

9.30. Desarrollo externalizado [ISO 27001 A.8.30]

Cuando se reciban las modificaciones a los sistemas registrales o administrativos a cargo de la Sede Central dentro del alcance del SGSI la Unidad de Tecnologías de la Información deberá verificar que se implementaron los requisitos y recomendaciones de seguridad de la información que fueron solicitados, para lo cual deberá hacer las pruebas correspondientes.

De verificar que no se han implementado dichos requisitos se deberá preparar un documento dirigido a la Oficina de Tecnologías de la Información comunicando este hecho.

En el caso de nuevas funcionalidades, nuevos aplicativos o nuevos sistemas de información, la Unidad de Tecnologías de la Información (UTI) deberá hacer un análisis de la seguridad de la información de los mismos y remitir las recomendaciones de seguridad de la información a la Oficina de Tecnologías de la Información (OTI) de la Sede Central.

La OTI, al realizar mejoras a los sistemas dentro del alcance del SGSI a través de un tercero, no necesariamente solicita la opinión de la UTI. En ese sentido las recomendaciones de seguridad por parte de la UTI se realizarían luego de la implementación como una oportunidad de mejora.

9.31. Separación de los entornos de desarrollo, prueba y producción [ISO 27001 A.8.31]

Para la gestión, los ambientes lógicos en la zona registral, se tienen dos entornos Producción y Desarrollo.

Para otros pases a producción, como aplicaciones enlatadas (por ejemplo, software antivirus), si es posible brindar equipos virtuales (servidores y clientes) para pruebas.

9.32. Gestión del cambio [ISO 27001 A.8.32]

Los cambios que afecten la seguridad de la información, como cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información o de sistemas, deben considerar que el área usuaria que propone el cambio es responsable de su gestión y debe:

a) Identificar y evaluar los riesgos e implementar medidas de control. Esta evaluación de riesgos debe quedar documentada
b) Documentar todas las acciones realizadas para llevar a cabo el cambio.
c) Coordinar y comunicar con todas las unidades de organización involucradas y gestionar todas las autorizaciones correspondientes.
d) Realizar un planeamiento que puede materializarse en un cronograma coordinado y comunicado con todas las partes interesadas.
e) Establecer un procedimiento de vuelta atrás en caso que el cambio no tenga éxito o exista un evento imprevisto.
f) En caso de afectar a los servicios informáticos, debe coordinar con UTI.

La gestión de interrupción programada de los servicios informáticos se debe seguir según lo indicado en los “Lineamientos para la gestión de interrupción programada de los servicios informáticos en las Zonas Registrales de la Superintendencia Nacional de los Registros Públicos (Sunarp)”.

La gestión de cambios de los sistemas informáticos se realiza según lo indicado en el “Procedimiento de Desarrollo, Mantenimiento y Seguridad de Programas”.

La gestión de cambios por incidentes disruptivos no planificados se realiza según lo indicado en el “Procedimiento de Gestión de Incidentes Disruptivos del Plan Recuperación Tecnológica ante Desastres”.

La gestión de cambios por las pruebas y ejercicios de las Instalaciones de procesamiento de la información y su respectivo equipamiento se realiza según lo indicado en el “Procedimiento de Ejercicios y Pruebas del Plan de Recuperación Tecnológica ante Desastres”.

9.33. Información de la prueba [ISO 27001 A.8.33]

NO APLICA,

debido a que el desarrollo de los sistemas de información incluidos en el alcance, se realizan en la Sede Central.

9.34. Protección de los sistemas de información durante las pruebas de auditoría [ISO 27001 A.8.34]

a) Se debe 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.

ANEXO N°1: MODELO DE LA CLÁUSULA DE CONFIDENCIALIDAD

EL (LA) CONTRATISTA/PROVEEDOR (A) se compromete a respetar y aplicar en la ejecución de las labores del presente contrato/orden de servicio, las políticas, los procedimientos, los estándares y los controles de seguridad de la información establecidos por la Zona Registral N° IX (LA ENTIDAD) los mismos que declara conocer y aceptar.

EL (LA) CONTRATISTA/PROVEEDOR (A) deberá proteger los activos de información (información, software, hardware físicos, documentación, entre otros) de la Zona Registral N° IX (LA ENTIDAD) de acceso no autorizado, pérdida, modificación y/o destrucción, falsificación, robo, uso Indebido y/o divulgación no autorizada.

EL (LA) CONTRATISTA/PROVEEDOR (A) se obliga a mantener y guardar estricta reserva y absoluta confidencialidad de todos los documentos o informaciones de la Zona Registral N° IX (LA ENTIDAD) a los que tenga acceso en ejecución del presente contrato/orden de servicio. Se entiende que la obligación asumida por EL (LA) CONTRATISTA/PROVEEDOR (A) está referida no solo a los documentos e informaciones señalados como “confidenciales” sino a todos los documentos o informaciones que en razón del presente contrato/orden de servicio o vinculado con la ejecución del mismo pueda ser conocida por cualquier medio por EL (LA) CONTRATISTA/PROVEEDOR (A). En consecuencia, EL (LA) CONTRATISTA/PROVEEDOR (A) deberá abstenerse de divulgar tales documentos, conversaciones, acuerdos de reuniones y comentarios que como parte de la función son de uso conocimiento, sea en forma directa o indirecta.

EL (LA) CONTRATISTA/PROVEEDOR (A) solo podrá revelar al personal que estrictamente sea necesario para la realización de las actividades materia del presente contrato/orden de servicio, los documentos e informaciones a los que se refiere el numeral precedente.

En el caso que EL (LA) CONTRATISTA/PROVEEDOR (A) fuera requerido (a) por alguna autoridad administrativa o judicial para revelar la información y/o documentación a la que se refiere la presente clausula, EL (LA) CONTRATISTA/PROVEEDOR (A) deberá notificar anticipadamente a la Zona Registral N° IX (LA ENTIDAD) para que esta adopte las medidas que considere necesarias para proteger la confidencialidad de la información. Se deja expresamente establecido que el deber de confidencialidad o suscripción del presente contrato/orden de servicio se extiende incluso hasta después del cese de la relación contractual con la organización por el lapso de … (colocar el tiempo de confidencialidad requerido por el área usuaria – 00 meses o años).

EL (LA) CONTRATISTA/PROVEEDOR (A) se compromete a devolver todo activo (software, documentación, equipos, claves de acceso, entre otros) que le haya proporcionado la Zona Registral N° IX (LA ENTIDAD) para el desempeño de sus funciones al momento de resolución o término del presente contrato/orden de servicio, sin que sea necesario que éste se lo requiera.

El incumplimiento de las obligaciones que asume EL (LA) CONTRATISTA/PROVEEDOR (A) en las cláusulas precedentes constituye la resolución del presente contrato/orden de servicio, de conformidad con lo previsto en el ***artículo 68° de la Ley N° 32069, Ley General de Contrataciones Públicas***, sin perjuicio de la obligación de EL (LA) CONTRATISTA/PROVEEDOR (A) de pagar a la Zona Registral N° IX (LA ENTIDAD) la indemnización correspondiente.”

CUADRO DE CONTROL DE CAMBIOS

Ítem	Descripción del cambio	Código / Versión
VII	Se modificó contenido en los numerales 7.1.1 Selección, 7.2.3 Procesos disciplinarios, 8.1.4. Retorno de redes	MN-001-JEF-ZRIX/V.04
VIII	Se modificó contenido en el numeral 8.1.4 Retorno de activos	
Del IV al XIV	Se modificó el presente manual para que se adecúe a la Directiva DI 001-OTI, denominada: ¨Directiva para el Acceso a la Plataforma de TICs¨	MA-001-2024-SUNARP-ZRIX-JEF/ V.05
VII	Se adicionó la legislación y normativa de teletrabajo en el 7.2.2	
VIII	Se adicionó en 8.1.1 que “Para la evaluación del personal encargado de las labores registrales se debe seguir lo establecido en el Reglamento de Acceso a la Función Registral dentro del Sistema Nacional de los Registros Públicos”	
VIII	Se indicó en 8.2.3 que el incumplimiento de alguna regulación establecida por el Sistema de Gestión de Seguridad de la Información es pasible de sanción.	
XIII	Se modificó el contenido de 13.1.2. Gestión de cambio y 13.1.3. Gestión de capacidad.	
XV	Se adicionaron controles para el dominio adquisición, de desarrollo y mantenimiento de sistemas, que anteriormente no estaban declarados en la Declaratoria de Aplicabilidad.	
XVI Anexo N°1	Se agrega un modelo de la cláusula de confidencialidad en el Anexo N°1 y se referencia en el 16.1.1	
XVII	Se modifica la 17.1.7 Recolección de evidencias.	
-	Documento reestructurado	MA-001-2024-SUNARP-ZRIX-JEF/ V.06

Anexo N° 1	Se modifica la referencia normativa por el artículo 68° de la Ley N° 32069, Ley General de Contrataciones Públicas	MA-001-2024-SUNARP-ZRIX-JEF/ V.07