MANUAL

POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SGSI-MA-03

ÍNDICE

1. OBJETIVO

Dar a conocer las políticas y lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI) de la Superintendencia Nacional de Aduanas y de Administración Tributaria – SUNAT, necesarios para implementar los controles establecidos en el Anexo A de la NTP-ISO/IEC 27001:2014, los cuales permiten alcanzar los objetivos definidos para la seguridad de la información de la institución.

2. ALCANCE

Las políticas que se contemplan dentro del presente documento aplican a todos los colaboradores, personal de modalidades formativas y terceros vinculados que gestionen información de la institución.

3. REFERENCIAS NORMATIVAS

- ISO/IEC 27000:2014. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Visión general y vocabulario.
- NTP-ISO/IEC 27001:2014. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2a. Edición.
- ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.
- Resolución Ministerial Nº 004-2016-PCM, que aprueba el uso obligatorio de la NTP-ISO/IEC 27001:2014, en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial N° 166-2017-PCM, que modifica el artículo 5 de la Resolución Ministerial Nº 004-2016-PCM.

4. DEFINICIONES Y ABREVIATURAS

4.1. Activo de Información: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de

la misma (sistemas, soportes, equipamiento informático, edificios, personas, etc.) que tenga valor para la organización.

4.2. **Activo de Información Crítico:** Se refiere a la información, o cualquier activo de información, que se considera indispensable para el correcto funcionamiento de la organización y sus procesos. Como parte de esta definición, en el documento se puede hacer mención a documentos, sistemas de información, ambientes físicos, entre otros.

4.3. **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a personas , entidades o procesos no autorizados.

4.4. **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una persona, entidad o proceso autorizado.

4.5. **Dispositivo móvil:** Es un equipo que permite que sea transportado con frecuencia y facilidad de un lugar a otro y tenga la capacidad de comunicación inalámbrica, por ejemplo: laptop, smartphone, tablet u otros similares.

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

4.7. **Evento de Seguridad de la Información:** Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

4.8. **Incidente de Seguridad de la Información:** Un solo evento o una serie de eventos de seguridad de la información, inesperados o no deseados, que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

4.9. **Información:** Conjunto de datos contenidos en documentos físicos (papel, microfichas, libros, etc.), medios magnéticos (cintas, discos, etc.), medios ópticos (CD, DVD, etc.) y medios electrónicos (USB, disco duro externo, etc.), que poseen valor para la entidad.

4.10. **Integridad:** Propiedad de la información relativa a su exactitud y completitud.

4.11. Propietario del Activo de Información: Persona o entidad que tiene la responsabilidad gerencial aprobada de controlar la producción, recepción, desarrollo, mantenimiento, uso y seguridad de los activos. Tiene autoridad formal y no significa que tenga derechos de propiedad sobre el activo.

4.12. Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información cualquiera sea su formato y soporte. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.

4.13. Sistema de Información: Conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes que manejan la información.

4.14. Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

4.15. Usuario de la Información: Persona autorizada a utilizar un sistema de información determinado, bajo un nivel de acceso preestablecido. Para efectos del presente documento, se refiere a los colaboradores, personal de modalidades formativas y terceros vinculados con la SUNAT.

ABREVIATURAS

- **EGR:** Equipo de Gestión de Riesgos.
- **GSI:** Gerencia de Seguridad de la Información.
- **INRH:** Intendencia Nacional de Recursos Humanos.
- **INSI**: Intendencia Nacional de Sistemas de Información.
- **OFSI:** Oficial de Seguridad de la Información.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **SUNAT:** Superintendencia Nacional de Aduanas y de Administración Tributaria.

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

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

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

a. Las políticas de seguridad de la información establecen las directivas y requerimientos necesarios para implementar un razonable nivel de protección de los activos de información de la SUNAT.

b. Se ha establecido una política general de seguridad de la información en el documento Política de Seguridad de la Información (SGSI-PO-01), así como políticas específicas documentadas en el presente documento.

c. Las políticas de seguridad son aprobadas, publicadas y comunicadas según lo definido en el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01).

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

La revisión de las políticas de seguridad de la información se realizan según lo definido en el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01).

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

6.1. ORGANIZACIÓN INTERNA [ISO 27001 A.6.1]

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

Los roles y responsabilidades del personal y terceros de la SUNAT con respecto al SGSI, han sido definidas en el Manual de Roles, Responsabilidades y Autoridades Organizacionales del SGSI (SGSI-MA-02).

6.1.2. Segregación de funciones [ISO 27001 A.6.1.2]

a. Toda área de la SUNAT debe solicitar los accesos para su personal alineado a sus labores y funciones documentadas o necesidad operativa, evitando cualquier conflicto para una correcta segregación de funciones.

b. La responsabilidad de los propietarios de los activos de información debe ser autorizar los accesos a la información teniendo en consideración:

- Una adecuada definición y segregación de funciones, de acuerdo a las actividades y funciones operativas que deban cumplir los distintos usuarios
- La sensibilidad de los datos
- La oposición de intereses entre las áreas afectadas.

c. Resultará necesario determinar una declaración de perfiles de usuarios y los mismos estarán determinados por grupos específicos para cada sistema de información.

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

a. Los Intendentes, Gerentes o Jefes de las UUOO deben establecer internamente, el mecanismo para recurrir a una instancia técnica de apoyo o asesoría en temas relacionados con la seguridad de la información que gestionan.

b. Asimismo, se debe mantener una lista con los teléfonos de los Bomberos, Policía, Hospitales y contacto con entidades reguladoras que les correspondan.

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

a. El personal de la SUNAT involucrado en la gestión de la seguridad de la información y la seguridad informática debe establecer los contactos en foros o grupos especializados que les permita recibir novedades y actualizaciones respecto a la seguridad de la información, y debe mantener constante relación con las entidades

externas que puedan prestar apoyo en caso de incidentes de seguridad de la información; la relación deberá mantenerse a un nivel tal que asegure el apoyo, pero sin generar obligaciones de entregar información confidencial o restringida.

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

a. La seguridad de la información debe integrarse en el método de gestión de proyectos de la SUNAT para garantizar que los riesgos de seguridad de la información sean identificados y tratados como parte de un proyecto.
b. La evaluación de riesgos de seguridad de la información debe realizarse en una etapa temprana del proyecto para identificar los controles necesarios.

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

6.2.1. Política de dispositivos móviles [ISO 27001 A.6.2.1]

a. La SUNAT ha establecido la presente Política de Dispositivos Móviles:
    - Todos los dispositivos móviles deben contener la última o la más segura versión de los productos de software. Los parches o actualizaciones deben ser obtenidos por la INSI de manera formal, provenientes del fabricante.
    - Los usuarios que utilicen computadores portátiles en su puesto de trabajo, para el cumplimiento de las funciones asignadas, deben mantener el equipo asegurado con cadena o en algún mueble con llave.
    - Los usuarios deben asegurarse de no dejar desatendidos los dispositivos móviles sin ningún bloqueo de acceso.
    - La INSI debe mantener actualizado el software antivirus de los dispositivos móviles.
    - El Propietario del Activo de Información (dispositivo móvil) debe verificar que los dispositivos móviles tengan habilitadas

las políticas de seguridad definidas por el área competente para estos equipos.

6.2.2. Teletrabajo [ISO 27001 A.6.2.2]

a. El servicio de acceso remoto debe permitir el acceso a la red de datos a aquellos usuarios internos expresamente autorizados por el Intendente, Gerente o Jefe de la UUOO.
b. El servicio de acceso remoto debe permitir el acceso a la red de datos a aquellos usuarios externos expresamente autorizados por el Intendente, Gerente o equivalente, con visto bueno del Jefe de la Oficina de Seguridad Informática. El acceso desde redes externas o internas deberá considerar la autenticación con un nivel adecuado de protección y obedecer a necesidades justificadas.
c. Solo los equipos de procesamiento de datos tipo servidor y de comunicación deben tener habilitado el servicio de conexión de acceso remoto y en casos que lo requieran, previa autorización y justificación, se habilitará el servicio de conexión de acceso remoto en otros equipos. Los usuarios para acceder a estos recursos serán previamente identificados y autorizados.
d. Cualquier usuario que requiera acceso a la red desde el exterior, debe estar debidamente autenticado y sus conexiones estarán encriptadas.

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

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

7.1.1. Selección [ISO 27001 A.7.1.1]

a. La INRH debe mantener listas de verificación de todos los candidatos a colaboradores, en concordancia con las leyes, regulaciones, ética y requerimientos de la SUNAT. Dichas listas deben tomar en consideración, la privacidad y la protección de los datos del candidato, incluyendo lo siguiente:
    - La disponibilidad de referencias suficientes.

- La comprobación de los documentos de identificación como, por ejemplo, currículo vitae, certificados académicos y profesionales.
- Comprobaciones más detalladas, por ejemplo: antecedentes penales y/o, policiales.

b. Para la evaluación de los candidatos a colaboradores de la SUNAT, la INRH debe seguir los lineamientos establecidos por la institución.

7.1.2. Términos y condiciones del empleo [ISO 27001 A.7.1.2]

a. Los contratos laborales deben incluir una sección en la cual se especifiquen las responsabilidades del empleado respecto a la seguridad de la información de la SUNAT.
b. La definición debe incluir el tipo de acciones que se tomen cuando se incumpla este requerimiento. Adicionalmente deben estar acordados las responsabilidades y derechos legales del empleado en cuanto a aspectos de privacidad y protección de datos personales y leyes aplicables.
c. La INRH debe definir los términos y condiciones del empleo del personal de la SUNAT.

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

7.2.1. Responsabilidades de la gerencia [ISO 27001 A.7.2.1]

a. El Oficial de Seguridad de la Información debe coordinar con la INRH y/o con diferentes áreas (cuando estas contratan terceros para servicios) los aspectos relacionados con los empleados que ingresen a trabajar a la SUNAT para que conozcan sus roles y responsabilidades con respecto a la seguridad de la información.
b. Todos los Intendentes, Gerentes o Jefes de las UUOO deben asegurar el cumplimiento por parte del personal y terceros a su cargo, de las políticas y procedimientos de seguridad de información establecidos en la institución, así como sus roles y responsabilidades.

c. Los Intendentes, Gerentes o Jefes de la UUOO que requieran de servicios de terceros, deben asegurar que a todo tercero, se le defina sus responsabilidades en la selección del personal y que sea informado respecto a las políticas y procedimientos de seguridad de la información vigentes. Asimismo, las UUOO según sus competencias, deberán tomar las medidas necesarias para que dicho servicio se realice de conformidad con las políticas de seguridad institucionales.

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

a. Se deben realizar charlas de inducción y sensibilización al personal de la SUNAT donde se difundan los temas de seguridad de la información, su contribución a la eficacia del SGSI incluyendo los beneficios de un mejor desempeño y, las consecuencias del incumplimiento de los requisitos establecidos en el SGSI. La asistencia por parte del personal debe ser registrada.
b. La concientización, educación y capacitación del SGSI debe ser gestionada por el Oficial de Seguridad de la Información de acuerdo al Plan de Capacitación y Sensibilización Integral en Seguridad de la Información (SGSI-PL-01) y en coordinación con la INRH.

7.2.3. Procesos disciplinarios [ISO 27001 A.7.2.3]

a. La SUNAT debe establecer que se procederán a sanciones disciplinarias en caso de identificarse violaciones a las normas emitidas por la Institución, las que incluyen las políticas y procedimientos relacionados con la seguridad de la información de la entidad, según lo definido en el Reglamento Interno de Trabajo, el cual considera faltas disciplinarias sujetas a sanción el incumplir las disposiciones laborales vigentes y las normas emitidas por la SUNAT.

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

7.3.1. Terminación o cambio de responsabilidades del empleo [ISO 27001 A.7.3.1]

a. Las responsabilidades para realizar la finalización del empleo de un colaborador o el cambio de éste, deben ser claramente definidas, asignadas y comunicadas por la INRH.
b. La INRH debe ser responsable del proceso de finalización del empleo del colaborador para lo cual debe trabajar conjuntamente con el Intendente, Gerente o Jefe del colaborador cesante y, de ser requerido con el Oficial de Seguridad de la Información.
c. El responsable de la INRH debe informar oportunamente a los involucrados en los procesos de ceses sobre el fin de contrato del personal con la SUNAT, para tomar las medidas preventivas y correctivas necesarias.
d. Los Intendentes, Gerentes o Jefes de cada área deben informar oportunamente a la INRH y a la INSI sobre los ceses imprevistos de personal.
e. La comunicación de la finalización de las responsabilidades debe incluir requisitos de seguridad de la información, responsabilidades legales y, donde sea apropiado, responsabilidades contenidas dentro de cualquier acuerdo de confidencialidad; asimismo las responsabilidades y tareas que son todavía válidas después de la finalización del empleo deben ser contenidas en dicha comunicación.
f. La INRH debe ser responsable del proceso de rotación del personal para lo cual debe trabajar conjuntamente con el Jefe anterior y Jefe nuevo del colaborador que cambia de responsabilidades del empleo y, de ser requerido, con el Oficial de Seguridad de la Información.
g. La INRH debe informar a la INSI sobre el cambio de funciones o de área del personal de la SUNAT.
h. La INSI debe realizar el cambio en los accesos de acuerdo a los perfiles de usuario definidos en los procedimientos vigentes para la solicitud y atención de cuentas de acceso.
i. Las actividades asociadas al alta, baja y modificación de usuarios de los sistemas informáticos de la SUNAT deben realizarse de acuerdo

a los procedimientos vigentes para la solicitud y atención de cuentas de acceso.

8. GESTIÓN DE ACTIVOS (ISO 27001-A.8)

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

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

a. Se debe registrar y mantener actualizados los activos de información que están involucrados en los procesos que forman parte del alcance del SGSI en el documento Inventario de Activos de Información (SGSI-ME-01.FO-01).

b. Para el desarrollo del Inventario de Activos de Información se debe realizar lo especificado en el documento Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01).

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

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

b. El propietario del activo de información se debe registrar en el Inventario de Activos de Información, según lo detallado en el documento Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01).

c. La SUNAT es el propietario de los activos de información de la entidad y debe delegar dicha propiedad a los Intendentes, Gerentes o Jefes de las UUOO con la finalidad de descentralizar y mejorar la eficiencia en la administración de la seguridad de información.

d. Los Intendentes, Gerentes o Jefes de las OOUU también podrían delegar la propiedad de los activos de información de manera jerárquica a los colaboradores a su cargo, manteniendo los Intendentes, Gerentes o Jefes de las UUOO, la responsabilidad ya asignada sobre los activos.

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

a. El uso aceptable de todos los activos de información de la SUNAT debe ser ejercido por todos los colaboradores y personal de modalidades formativas con el propósito expreso de realizar tareas relacionadas a las actividades de la institución.
b. Los activos de información deben ser utilizados por todos los colaboradores y personal de modalidades formativas dentro de un adecuado entorno de seguridad, cualquiera sea el medio que los soporte y el ambiente tecnológico en que se procesen.

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

a. La finalización del empleo debe incluir el retorno previo de los activos de información proporcionados por la SUNAT al colaborador o tercero (de ser el caso) para el desempeño de las funciones asignadas.
b. La devolución de activos tecnológicos, así como la eliminación de la información contenida en los mismos, se debe realizar de acuerdo a los documentos vigentes y de manera segura.

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

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

a. La información debe clasificarse según su sensibilidad o grado de impacto en el negocio, según los siguientes niveles:
    - **Público:** Son activos que se consideran públicos y que pueden ser accedidos tanto por miembros de la entidad como por personas externas a ella (público en general), sin estar sujetos a ningún control.
    - **Uso Interno:** Son activos que son accedidos exclusivamente por personal interno de la entidad y cuyo acceso excepcional por parte de personal externo (auditores, entidades reguladoras, consultores externos) puede darse, pero se encuentra regulado y sujeto a condiciones específicas de acceso.
    - **Confidencial:** Son activos que pertenecen a un proceso que por su naturaleza son reservados exclusivamente al personal del proceso específico y cuyo acceso excepcional por parte de

personal externo (auditores, entidades reguladoras, consultores externos) puede darse pero se encuentra regulado y sujeto a condiciones específicas de acceso. Su revelación requiere la aprobación de su dueño o propietario, es de uso exclusivo de la organización, en el caso de terceros se deberá firmar acuerdo de confidencialidad y no divulgación.

- **Restringida:** Son activos cuyo acceso es restringido a un grupo determinado de individuos, seleccionados a partir de un proyecto específico o que pertenecen a un grupo o nivel específico dentro de la entidad. Estos deben ser gestionados con todas las precauciones y controles posibles determinando exactamente que personas tienen acceso a los mismos y vigilando su uso, transporte y almacenamiento.

Esta clasificación debe estar especificada en el documento Metodología de Gestión de Riesgos de Seguridad de la Información (SGSI-ME-01).

b. Los usuarios de la SUNAT deben conocer la clasificación de la información.
c. Los propietarios de los activos de información deben ser responsables de la clasificación de la misma, en coordinación con el Oficial de Seguridad de la Información.

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

a. Teniendo en consideración los niveles mencionados en el punto anterior, el Propietario del Activo de Información debe asegurarse que todos los activos de información, fisicos o lógicos, deben estar debidamente etiquetados.
b. El marcado o rotulación de la información se debe realizar de manera estandarizada, de acuerdo a su clasificación.

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

a. Toda información documentada debe ser de uso exclusivo dentro de la SUNAT, salvo excepciones autorizadas.

b. Toda información documentada que sea crítica para la SUNAT, debe ser guardada en los repositorios de almacenamiento de información brindados por la institución.

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

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

a. Toda la información almacenada en medios removibles de la SUNAT debe estar debidamente controlada en cuanto a su uso, transporte y almacenamiento.

b. El control de medios removibles de almacenamiento (discos externos, cintas magnéticas) correspondientes al respaldo de información se debe realizar según lo especificado en los documentos vigentes.

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

En caso de desechar cualquier medio que contenga información confidencial o restringida, debe eliminarse de manera segura.

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

a. Cualquier información que deba ser trasladada desde la SUNAT a un sitio externo, deberá ser transportada en forma segura y controlada previa a su salida. Esto debe aplicar también para el almacenamiento de las copias de respaldo en sitios externos a la entidad.

b. El tratamiento que se les debe dar a los medios que almacenan activos de información de la SUNAT y que se trasladan fuera del ámbito de la entidad, se debe realizar según lo especificado en los procedimientos vigentes.

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

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

9.1.1. Política de control de acceso [ISO 27001 A.9.1.1]

a. Se ha establecido la presente Política de Control de Acceso:

- El control de acceso a los sistemas de información, a cargo de la INSI, debe realizarse por medio de códigos de identificación y contraseñas, únicos para cada usuario.

- Cada usuario debe contar con un identificador de usuario y una contraseña conocida sólo por dicho usuario (o grupo), mediante los cuales tendrá acceso a los sistemas de información autorizados, de acuerdo al perfil asignado por su área.
- El nivel de acceso a un sistema de información se otorgará de acuerdo a:
    - Funciones del usuario.
    - Perfiles de acceso estandarizados.
    - Solicitud, autorización y administración de acceso.
    - Segregación de funciones.
    - Revisión periódica de privilegios.
- Los sistemas de información se deben desconectar automáticamente tras un período definido de inactividad que sea configurable por cada sistema.
- Los sistemas de información se deben bloquear automáticamente después de un número máximo de intentos de acceso erróneos a fin de evitar ataques cibernéticos. El número máximo de intentos, así como el periodo transcurrido entre cada intento, debe ser configurable por cada sistema.
- Cada usuario solo podrá tener una sesión abierta por aplicación.
- La sesión debe expirar cuando se cierra el navegador.
- Toda aplicación informática deberá estar inscrita ya sea en el Menú Intranet o en el Menú SOL, según corresponda.
- Toda aplicación informática deberá generar logs para intentos fallidos de inicio de sesión.
- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información debe ser asignado de acuerdo a la identificación previa de los requisitos de seguridad, y de los marcos regulatorios vigentes aplicables.
- Los equipos de cómputo deben ser asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.

- En lo posible se deben usar sistemas o técnicas criptográficas para proteger la información crítica y sometida a alto riesgo, cuando otras medidas o controles no proporcionen la protección adecuada.

b. La presente política debe estar soportada por procedimientos formales y responsabilidades definidas, los cuales se deben registrar en los documentos vigentes.

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

a. Se deben establecer diferentes segmentos de red, dependiendo de la criticidad de las aplicaciones.

b. Las acciones y controles necesarios para monitorear el uso de los medios de procesamiento, detectar posibles fallas y analizarlas para tomar las acciones apropiadas se deben realizar según lo establecido en los procedimientos vigentes. Los cuales deberán contemplar como mínimo:

- Los perfiles de acceso y directivas de acceso lógico deben considerar los servicios de red y conexiones a las redes a los que un usuario puede tener acceso.
- Se debe considerar la verificación de los medios usados (Token, entre otros) para el acceso a los servicios de red.
- Se deben implementar mecanismos de identificación de un usuario que se conecta remotamente a la red de la organización.
- El acceso remoto a la red de SUNAT se debe realizar de acuerdo a los procedimientos vigentes.
- Se debe implementar control de ruteo de redes para asegurar que las conexiones y los flujos de información entre computadores no violen las políticas de control de acceso de las aplicaciones de la SUNAT.
- Para la conexión de equipos a la red se debe considerar:
  - Limitar y registrar el número de intentos fallidos de conexión, luego de lo cual el usuario debe quedar deshabilitado por un periodo de tiempo.

- Limitar el tiempo de la conexión, luego del cual el usuario deberá autenticarse nuevamente.
- Contar con identificadores de los equipos que se conectan a la red. Estos identificadores deben ser asignados según los lineamientos establecidos.

c. Las actividades asociadas al alta, baja y modificación de usuarios de los sistemas informáticos de la SUNAT se deben realizar según los procedimientos vigentes para la solicitud y atención de cuentas de acceso.

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

9.2.1. Registro y baja de usuario [ISO 27001 A.9.2.1], Aprovisionamiento de acceso a usuario [ISO 27001 A.9.2.2], Gestión de información de autenticación secreta de usuarios [ISO 27001 A.9.2.4], Remoción o ajuste de derechos de acceso [ISO 27001 A.9.2.6]

a. La INSI debe establecer un conjunto de controles y procedimientos con el fin de obtener un alto nivel de seguridad en la gestión de contraseñas y usuarios de los sistemas informáticos de la entidad.

b. Todas las cuentas de acceso deben solicitarse con relación a las funciones que corresponden a cada usuario y tomando en consideración los perfiles y opciones que se definan para cada aplicación, minimizando la creación de cuentas por usuario para un adecuado control.

c. Las cuentas de acceso que se asignan son personales, confidenciales e intransferibles, por lo tanto no deben ser compartidas y toda acción que se realice con ellas es responsabilidad del usuario titular.

d. Las cuentas de acceso deben ser usadas única y exclusivamente para actividades relacionadas con el cumplimiento de las funciones asignadas por la Institución a través del uso del sistema en producción requerido y autorizado. No pueden ser usadas para propósitos distintos, ilegales o no éticos.

e. Las peticiones de alta, baja y/o modificación de las cuentas de accesos a los sistemas de información deben ser autorizadas por las

jefaturas inmediatas y atendidas por la INSI, y se deben realizar según los procedimientos vigentes para la solicitud y atención de cuentas de acceso.

f. Un identificador de usuario eliminado no se debe volver a asignar a otra persona en el futuro.
g. En los casos de ceses y licencias de personal, los permisos y accesos a los sistemas de información deben ser retirados o bloqueados según tiempo indicado.
h. En los casos de rotación del personal, los permisos y accesos a los sistemas de información deben ser cambiados, de acuerdo al nuevo rol que ejercerá el empleado, previa gestión del Intendente, Gerente o Jefe de la UUOO.
i. El área encargada de la INSI debe administrar y llevar el control de la gestión de los accesos y validar la deshabilitación de los accesos en los principales sistemas del personal cesado.

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

a. El control del correcto uso y disposición de contraseñas de los diversos sistemas informáticos involucrados en la operación, considerados críticos para el negocio y en particular sobre el control de acceso lógico a plataformas y sistemas de red se deben realizar según lo establecido en los procedimientos vigentes.
b. Toda cuenta de administrador o de altos privilegios debe ser solicitada con el sustento necesario y según lo establecido en los procedimientos vigentes para la solicitud y atención de cuentas de acceso.
c. Las actividades regulares de un usuario no deben ser realizadas desde cuentas privilegiadas.

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

a. Los Intendentes, Gerentes o Jefes de la UUOO de la SUNAT en coordinación con el área encargada de la INSI, deben revisar periódicamente los derechos de acceso, revocando los que hayan caducado, los que no estén siendo utilizados o ya no correspondan

con la función desempeñada por cada empleado, según lo establecido en el procedimiento vigente para la solicitud y atención de cuentas de acceso.

9.3. RESPONSABILIDADES DE LOS USUARIOS [ISO 27001 A.9.3]

9.3.1. Uso de información de autentificación secreta [ISO 27001 A.9.3.1], Sistema de gestión de contraseñas [ISO 27001 A.9.4.3]

a. Las contraseñas de acceso deben ser cambiadas por lo menos cada seis (6) meses, a excepción de las cuentas de red para el ingreso al dominio SUNAT que tienen un tiempo de vida de noventa (90) días y para las cuales el sistema solicita el cambio de contraseña.

b. Las contraseñas son confidenciales, personales e intransferibles, por lo tanto, en caso se detecte que un usuario mantiene la contraseña de una cuenta que no le ha sido asignada, con o sin consentimiento del usuario titular, será notificado por la INSI a la INRH para que tome las acciones que correspondan.

c. Los usuarios titulares de cuentas de acceso son responsables de mantener la confidencialidad, privacidad y el secreto de sus contraseñas, por tal motivo, éstas no deben ser compartidas con otra persona y no deben ser escritas en ningún papel o archivo.

d. Para la creación y cambio de contraseña, debe tomarse en consideración las recomendaciones siguientes:

- En caso de cuentas de sistemas, la contraseña debe tener, por lo menos, seis (6) caracteres y, en caso de cuentas de red, la contraseña debe tener, por lo menos, doce (12) caracteres. Ambas deben estar compuestas de caracteres en mayúscula y minúscula, números y caracteres especiales.
- No debe considerarse nombres o palabras comunes, ni datos personales.
- Al cambiarla, no debe considerarse las últimas dos (2) contraseñas utilizadas.
- En el caso de las cuentas genéricas, la extensión de las contraseñas de acceso deben tener, por lo menos, doce (12)

caracteres y, de ser posible, diferentes para cada sistema y por cada servidor o cada instancia de base de datos.

En el caso de cuentas genéricas asignadas a la ejecución de procesos, el área encargada del soporte y operación de la infraestructura tecnológica de la INSI es responsable de realizar dicha acción.

e. Las contraseñas temporales o por defecto deben ser enviadas a los usuarios de manera segura y directa. Los usuarios tienen la responsabilidad de cambiar dichas contraseñas inmediatamente una vez recibidas y verificadas.
f. De existir sospecha del uso de la cuenta por un tercero, el usuario titular debe cambiar inmediatamente la contraseña de acceso y comunicar al área encargada de la Seguridad Informática como un evento de seguridad de la información.
g. No se deben incluir las contraseñas en ningún mecanismo automático de conexión que las deje almacenadas en el equipo.

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

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

a. El propietario de los activos de información debe establecer que los usuarios tendrán derecho a acceder a la información según el perfil de usuario asignado y el nivel de clasificación de dicha información. En la generación de perfiles, se debe controlar los derechos de acceso a lectura, escritura, borrado y ejecución analizado entre la INSI y el área usuaria.
b. Esta prohibido el traslado o almacenamiento de información de la SUNAT en sitios web que ofrezcan servicios de almacenamiento de información y/o convertidor de formatos de documentos. Las herramientas de productividad informática, entre las que se incluyen las de almacenamiento de información en la nube, están establecidas en el Lineamiento de Herramientas de Productividad Informáticas Office 365 (A03.2-LT-001) vigente, establecido por la INSI.
c. Esta prohibida la creación de carpetas compartidas en modo público, con todos los privilegios, en la red de la SUNAT. Las carpetas

compartidas sólo deben ser creadas por el área encargada del soporte y operación de la infraestructura tecnológica de la INSI, y no deben tener acceso público. Es responsabilidad de todos los colaboradores y personal de modalidades formativas que hayan solicitado la creación de una carpeta compartida, establecer un límite de acceso y mantener dicha restricción con las personas autorizadas.

9.4.2. Procedimientos de ingreso seguro [ISO 27001 A.9.4.2]

El personal debe asumir el compromiso y responsabilidad al recibir su contraseña y su nombre de usuario. Adicionalmente, los usuarios deben proteger el acceso a su estación de trabajo activando el protector de pantalla o haciendo un logout del sistema.

9.4.3. Uso de programas utilitarios privilegiados [ISO 27001 A.9.4.4]

En la SUNAT debe restringirse y controlarse estrechamente el uso de programas utilitarios que pudieran ser capaces de anular los controles del sistema y las aplicaciones.

9.4.4. Control de acceso al código fuente de los programas [ISO 27001 A.9.4.5]

a. Se debe restringir y controlar el acceso al código fuente de los programas únicamente al personal autorizado para su edición y/o modificación.
b. Se debe de implementar un proceso automático y/o manual que permita controlar el versionamiento del código fuente.
c. Si se trata de una aplicación desarrollada por un proveedor externo, se deben revisar las condiciones del contrato.

10. CRIPTOGRAFÍA (ISO 27001-A.10)

10.1. CONTROLES CRIPTOGRÁFICOS [ISO 27001 A.10.1]

10.1.1. Política sobre el uso de controles criptográficos [ISO 27001 A.10.1.1]

a. Se ha establecido la presente Política sobre el Uso de Controles Criptográficos:

- Se deberán utilizar controles criptográficos en los siguientes casos:
    - Para la transmisión de información clasificada como confidencial o restringida, fuera de la entidad.
    - Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario del Riesgo.
- La INSI debe desarrollar lineamientos respecto de la administración de contraseñas, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las contraseñas y en cuanto al reemplazo de las contraseñas de cifrado.

10.1.2. Gestión de claves [ISO 27001 A.10.1.2]

a. Las llaves criptográficas utilizadas para el cifrado de los datos deben estar clasificadas como confidencial y deben ser protegidas contra divulgación, uso indebido o sustitución no autorizada restringiendo al mínimo el número de custodios necesarios y guardándola de forma segura en la menor cantidad de ubicaciones y formas posibles.
b. Para reducir la probabilidad de compromiso, las llaves deben tener fechas de inicio y caducidad de vigencia.

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

11.1. ÁREAS SEGURAS [ISO 27001 A.11.1]

11.1.1. Perímetro de seguridad física [ISO 27001 A.11.1.1], Controles de ingreso físico [ISO 27001 A.11.1.2], Asegurar oficinas, áreas e instalaciones [ISO 27001 A.11.1.3]

a. Se debe establecer el registro de todo ingreso y egreso del personal interno y visitantes que deban acceder a diferentes sitios de la entidad. Este control deberá estar establecido mediante el uso de fotocheck o pase, según corresponda, que se deberá portar en todo momento.
b. El acceso a las diferentes áreas de la SUNAT debe estar estrictamente controlado a través de sistemas de control de acceso a

locales y de la asignación de las autorizaciones de ingreso correspondientes. No se debe permitir el ingreso de personal interno y terceros, sin las autorizaciones correspondientes o que no sigan el procedimiento establecido.

c. El personal de la SUNAT no debe 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.
d. El área encargada de la seguridad física de la SUNAT, debe garantizar y verificar que todas las puertas del Centro de Cómputo, además de tener instalados los controles electrónicos de acceso deben ser del tipo “cortafuego” con chapa anti pánico (fácil apertura ante emergencias).
e. El ingreso a los ambientes del Centro de Cómputo debe ser restringido.
f. La supervisión de las labores específicas del personal externo para el que fue autorizado al Centro de Cómputo, deberá estar a cargo del personal relacionado con el soporte especializado de dichos equipos previa autorización para su ingreso.
g. El área encargada de supervisar los Centros de Cómputo de la SUNAT, debe verificar y controlar el acceso y permanencia dentro del Centro de Cómputo a su cargo, del personal interno o externo cuyo ingreso haya sido autorizado para fines específicos, quienes deben portar el fotocheck institucional o pase otorgado en una parte visible de su vestimenta.
h. El personal del Centro de Cómputo o el personal autorizado que se encuentre en dicho Centro no debe acceder a la documentación y otros medios de almacenamiento de información óptico y/o magnético, ni a los recursos de su procesamiento si no está autorizado por el Supervisor o encargado del Centro de Cómputo.
i. El área encargada de supervisar los Centros de Cómputo de la SUNAT debe verificar y controlar que el Operador de Turno, ante una visita al Centro de Cómputo del personal interno o externo, registre el evento en el registro de control de acceso físico al Centro de

Cómputo. Este registro no deberá tener tachaduras ni enmendaduras y deberá estar protegido con las medidas de seguridad que corresponda, caso contrario se deberá validar la tachadura.

j. Para el acceso a los Centros de Cómputo de la SUNAT, se deben seguir los lineamientos establecidos en el documento vigente de normas y pautas para mantener la seguridad física, ambiental y de la información en los Centros de Cómputo de la SUNAT.
k. En lo posible, las oficinas deben quedar cerradas cuando no hay personas en su interior.
l. Los directorios y las guías o libretas telefónicas internas que identifiquen la ubicación de los recursos de información críticos no deben ser accesibles a personas no autorizadas.
m. Al dejar momentáneamente el sitio de trabajo o al finalizar la jornada, los escritorios y áreas de trabajo deben quedar desprovistos de documentos críticos. Estos deben quedar bajo llave en archivadores, credenzas, cajones u otros medios seguros.

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

a. Se debe contar con Certificado de Protocolo de Prueba de Puesta de Tierra e informe de las revisiones realizadas por el área encargada de los mantenimientos de las subestaciones eléctricas y sistemas de puesta a tierra a nivel nacional de la SUNAT.
b. El área encargada de la seguridad física de la SUNAT, debe verificar que en las inmediaciones de los Centros de Cómputo y áreas adyacentes a éstos, no se almacene ningún material inflamable (cajas de archivo documentario, equipos, accesorios y demás enseres).
c. Deben existir medios e información de respaldo ubicados a una distancia conveniente, en locaciones diferentes de los equipos principales.
d. El área encargada de la seguridad física de la SUNAT, debe realizar análisis de riesgo sobre posibles amenazas de desastres que puedan ocurrir en lugares próximos vecinos, tanto vertical como horizontalmente, que puedan afectar el funcionamiento de los Centros

de Cómputo y equipos de telecomunicaciones y recomendar las medidas preventivas.

e. Para evitar daños causados por desastres naturales, ataques maliciosos o accidentes, se debe seguir los lineamientos establecidos por el Área Encargada de la seguridad física de la SUNAT.

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

a. Los activos críticos de la SUNAT deben estar protegidos en áreas seguras para su operación, a través del uso de controles de acceso físico, reglamentos y sanciones; para lo cual se debe cumplir con las normas y procedimientos utilizados para asegurar la infraestructura y los activos de información que esta contiene.

b. El área encargada de supervisar los Centros de Cómputo de la SUNAT debe supervisar las labores del personal de limpieza así como del personal debidamente autorizado que realice mantenimientos preventivos y/o correctivos en el Centro de Cómputo a su cargo.

c. Se deben definir los lineamientos para el trabajo en áreas seguras, que considere:

- Que el personal encargado de la supervisión conozca de las actividades que se realizarán.
- Que las áreas seguras queden cerrados con llave si son desatendidas.
- Que no se permita el uso de equipos fotográficos, de audio o video, salvo previa autorización.

d. El ingreso a áreas de acceso limitado y restringido debe ser autorizado por los Intendentes, Gerentes o Jefes de las UUOO respectivas y supervisadas continuamente.

11.1.4. Áreas de despacho y carga [ISO 27001 A.11.1.6]

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

b. Las tareas de carga y descarga se realizarán en áreas de acceso público. Si se requiere del acceso a áreas internas, limitadas o restringidas, el Intendente, Gerente o Jefe de la UUOO respectiva debe autorizar y comunicar dicho acceso al agente de seguridad de turno.
c. El equipamiento o material entrante y saliente debe ser registrado de acuerdo a los lineamientos establecidos.

11.2. EQUIPOS [ISO 27001 A.11.2]

11.2.1. Emplazamiento y protección de los equipos [ISO 27001 A.11.2.1]

a. Se debe establecer que todos los equipos que se utilicen para el procesamiento de información de la entidad, deben contar con las medidas de protección para minimizar el riesgo de posibles amenazas físicas y ambientales.
b. Asimismo, los equipos deben contar con mecanismos que impidan y/o detecten los accesos o instalación no autorizada de componentes internos de hardware, así como mecanismos de control para el traslado de los mismos sin autorización. Todos los equipos deben contar con medidas de seguridad para evitar su pérdida, robo o fuga de información.
c. El área encargada de supervisar los Centros de Cómputo de la SUNAT debe hacer cumplir siempre las instrucciones del fabricante para proteger los equipos instalados en el Centro de Cómputo a su cargo para lo cual el personal del Centro de Cómputo deberá tener en cuenta el manual de los equipos instalados.

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

a. El área encargada del soporte y operación de la infraestructura tecnológica de la SUNAT, debe revisar y probar los equipos UPS, grupo electrógeno y tableros eléctricos de acuerdo a un cronograma y a las recomendaciones del fabricante para asegurar que tengan la capacidad adecuada. El mantenimiento de estos equipos debe garantizar la continuidad de los servicios que brinda la institución.

b. El área encargada del soporte y operación de la infraestructura tecnológica de la SUNAT, debe asegurar la disponibilidad del combustible necesario para el funcionamiento de los grupos electrógenos del Centro de Cómputo de San Isidro. La División de Mantenimiento (DIM) es la encargada del generador eléctrico de respaldo en los Centros de Cómputo de Lima y Callao. En los Centros de Cómputo de las sedes desconcentradas lo deberán hacer las Oficinas de Soporte Administrativo respectivas o la que cumpla sus funciones.

c. El área encargada del soporte y operación de la infraestructura tecnológica de la SUNAT, debe gestionar la capacitación requerida al personal que labora en los centros de cómputo para que puedan activar los sistemas de desconexión en caso de emergencia, para lo cual deberán tener acceso a los tableros de electricidad. Asimismo, el área encargada de la seguridad física de la SUNAT, debe capacitar al personal que labora en los Centros de Computo sobre el uso, maniobras de los sistemas de extinción de incendios, alerta temprana, así como su funcionamiento y las medidas adoptar en caso de una emergencia.

d. El área encargada del soporte y operación de la infraestructura tecnológica de la SUNAT, en cada mantenimiento eléctrico periódico que realice, deberá efectuar previamente un inventario del estado de los equipos del Centro de Cómputo. Al finalizar el mantenimiento, deberá comprobar que ningún equipo eléctrico, electrónico o mecánico-eléctrico-electrónico del Centro de Cómputo haya sido dañado. Si el personal responsable de la área encargada del soporte y operación de la infraestructura tecnológica de la SUNAT detectara la existencia de fallas en el funcionamiento de cualesquiera de los equipos mencionados, reportará el hecho a la persona encargada del mantenimiento y mediante la herramienta de gestión de servicios de tecnología de información (HGSTI) a la Jefatura de la División de Mantenimiento de Infraestructura y Equipamiento para el análisis de la falla y su posterior trámite para los fines administrativos correspondientes.

e. Para proteger el equipamiento contra posibles fallas en el suministro de energía y/o servicios de apoyo, se debe seguir los lineamientos establecidos en el documento vigente de normas y pautas para mantener la seguridad física, ambiental y de la información en los Centros de Cómputo de la SUNAT.

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

a. El área encargada de soporte y operación de la infraestructura tecnológica, debe garantizar y verificar que las líneas de energía estén protegidas, en caso contrario debe adoptar las medidas alternativas de protección contra daños respecto al tipo de línea.
b. El área encargada de soporte y operación de la infraestructura tecnológica, debe garantizar que las bandejas del cableado de datos que se ubican por debajo del falso piso técnico permitan el flujo óptimo del aire acondicionado de los equipos que climatizan el Centro de Cómputo.
c. El área encargada de la gestión de la infraestructura tecnológica, debe garantizar y verificar que las líneas de transmisión de datos estén protegidas, en caso contrario deberá adoptar las medidas alternativas de protección contra daños o interceptaciones no autorizadas respecto al tipo de línea.
d. El área encargada de la gestión de la infraestructura tecnológica, debe garantizar y verificar que las líneas de transmisión de datos tendidas estén rotuladas, distribuidas y conectadas de acuerdo a las normas de cableado estructurado.
e. El área encargada de la seguridad física de la SUNAT, debe garantizar y verificar que las placas extraíbles del falso piso y falso techo sean de material no combustible, resistentes e impermeables. También debe asegurar que el área debajo del falso piso sea de fácil accesibilidad.
f. El cableado estructurado debe pasar periódicamente por un proceso de certificación que sea realizada por una entidad externa, especializada y certificada en la materia.

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

a. El mantenimiento de los equipos debe realizarse en forma adecuada para asegurar que su disponibilidad e integridad sean garantizados, teniendo en cuenta principalmente que el mantenimiento de equipos debe realizarse, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor, que sólo el personal de mantenimiento autorizado puede brindarlo y llevar a cabo reparaciones en el equipamiento y, por otra parte, que se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo. Además deben implementarse controles cuando se retiran equipos de la sede de la SUNAT para su mantenimiento.

b. El área encargada de supervisar los Centros de Cómputo de la SUNAT debe verificar que toda falla real o sospechosa de los equipos que se utilicen para el procesamiento de información sea registrada en la bitácora diaria, así como todo mantenimiento preventivo y correctivo efectuado; en el caso de servidores este registro deberá efectuarse en la hoja del ciclo de vida de cada equipo.

c. El área encargada de supervisar los Centros de Cómputo de la SUNAT debe supervisar los servicios de mantenimiento preventivo y/o correctivo de los equipos instalados en el Centro de Cómputo, el cual debe ser realizado sólo por el personal de mantenimiento debidamente autorizado.

d. El mantenimiento preventivo de equipos informáticos o suministros de soporte debe ser oportunamente comunicado.

e. El mantenimiento de equipos se debe realizar de acuerdo a lo establecido en el documento vigente de normas y pautas para el control del mantenimiento de los equipos informáticos administrados por la INSI.

11.2.5. Remoción de activos [ISO 27001 A.11.2.5]

Se debe establecer que los usuarios que requieran retirar activos de información fuera de las oficinas de trabajo habitual, deben estar autorizados por el Intendente, Gerente o Jefe de la OOUU al que

pertenecen dichos usuarios. Dada la naturaleza de la actividad de la SUNAT, se firmará un Acuerdo de Confidencialidad donde debe quedar claramente especificado, las responsabilidades por el manejo adecuado de dicha información.

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

a. Todos aquellos equipos, información, software o medios magnéticos que por motivos circunstanciales son utilizados fuera de la entidad, no deben salir sin una autorización formal previa.
b. El Propietario del Activo de Información, en coordinación con el Oficial de Seguridad de la Información, deben precisar el tipo de información que se puede mantener en este tipo de equipamiento.
c. El área encargada del soporte y operación de la infraestructura tecnológica de la SUNAT, debe asegurar que los equipos que tengan almacenada información que sean retirados de su entorno habitual, deben estar protegidos y no deben estar expuestos en sitios públicos. El cuidado y traslado de los equipos, así como los medios de almacenamiento deben efectuarse de acuerdo a las políticas y normas de uso adecuado de los equipos informáticos vigentes.

11.2.7. Disposición o reutilización segura de equipos [ISO 27001 A.11.2.7]

a. Todo equipamiento informático que contenga medios de almacenamiento debe revisarse para asegurar que todos los datos sensibles y software licenciado se haya eliminado de forma segura antes de su baja o reutilización.
b. Se debe realizar el borrado de información de cintas magnéticas, medios de almacenamiento óptico y equipos de la SUNAT, cuando estos equipos sean entregados o retirados por terceros para realizar una instalación por motivo de cambios o reparación. Esta actividad se debe realizar según lo especificado en los documentos formales de la entidad.

c. Debe verificarse el borrado de la información de los equipos informáticos que vayan a ser reutilizados o dados de baja, mediante mecanismos que aseguren que esta información no pueda ser recuperada por procesos técnicos.

11.2.8. Equipos de usuario desatendidos [ISO 27001 A.11.2.8]

a. Al dejar un equipo (estación de trabajo, dispositivo móvil y/o servidores) desatendido temporalmente, el usuario debe bloquear inmediatamente el acceso a los mismos, independientemente del tiempo que permanezcan alejados.
b. Al terminar la jornada de trabajo se debe apagar el equipo, siempre y cuando no se encuentren ejecutándose procesos programados fuera de horario de oficina y respondan a labores propias del cargo del colaborador. En caso de ausentarse de la oficina por un periodo prolongado de tiempo, se deben cancelar las sesiones de usuario dentro de las aplicaciones, además de bloquear la pantalla.
c. Se debe cerrar la sesión de administrador u operativo de los servidores cuando se ha concluido con la labor.

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

a. La información crítica impresa o almacenada de manera electrónica debe estar protegida de accesos no autorizados, especialmente cuando no estén siendo utilizados.
b. Una vez finalizada la tarea diaria, los usuarios no deben dejar hojas y papeles de trabajo sobre los escritorios. Asimismo, no deben dejar medios de almacenamiento desde donde se pueda obtener información de la entidad. El almacenamiento de estos elementos se debe realizar preferiblemente en gabinetes bajo llave.
c. Se debe tener especial cuidado con el uso de dispositivos como fotocopiadoras e impresoras, de manera tal que el material con información sensible no permanezca en las bandejas de dichos equipos sin atención y que no se utilice papel reciclado que contenga información confidencial o restringida. El acceso a impresoras,

escáneres, fotocopiadoras u otros similares debe ser bloqueado cuando se encuentren desatendidos.

d. La información impresa a eliminar debe ser desechada de manera segura y que no permita su reconstrucción total o parcial.

e. Para reducir el riesgo de acceso no autorizado a la información confidencial o restringida en los puestos de trabajo, se debe cumplir con el documento vigente de normas y pautas de pantallas y escritorios limpios.

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

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

12.1.1. Procedimientos operativos documentados [ISO 27001 A.12.1.1]

a. La INSI debe establecer que los procedimientos, registros y guías de trabajo se encuentren debidamente documentados con el fin de asegurar el mantenimiento y operación. Entre ellos:

- Se debe elaborar y mantener los procedimientos y las guías de usuarios finales, de configuración, de sistemas de información y recursos de comunicación.
- Se debe contar con los procedimientos documentados de los procesos de contingencia y respaldo de los sistemas o procesos de información crítica.
- Se debe tener identificado a los responsables de la operatividad de cada sistema de información, así como a los contactos de emergencia respectivos; dicha información debe ser actualizada según corresponda.

b. Para los procedimientos operacionales del SGSI, la creación y actualización de la información documentada deberán seguir los lineamientos definidos en el Procedimiento de Control de Información Documentada del SGSI (SGSI-PR-01).

12.1.2. Gestión del cambio [ISO 27001 A.12.1.2]

a. Todos los cambios en los sistemas de información, instalaciones de procesamiento o software base se deben realizar conforme a los

lineamientos respectivos de instalación, operación y mantenimiento, que permita identificar, registrar y controlar dichos cambios asegurando que no afectarán la confidencialidad, disponibilidad e integridad de la información. Estos cambios deben realizarse según los lineamientos definidos en los documentos vigentes, los cuales deben contemplar que los cambios sean autorizados, notificados oportunamente y aprobados.

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

a. La INSI debe proyectar y asegurar las demandas de capacidad de almacenamiento y procesamiento de información para evitar el bajo desempeño de los sistemas o perder información por el mal uso de los recursos informáticos actuales.
b. Se debe monitorear el uso de los recursos de TI para identificar y evitar su mal uso y problemas de mala configuración.

12.1.4. Separación de los entornos de desarrollo, pruebas y operaciones [ISO 27001 A.12.1.4]

a. La INSI deberá establecer que no se realicen pruebas, instalaciones o desarrollos sobre el entorno de producción. Se debe contar con ambientes separados para efectuar el desarrollo y mantenimiento de los sistemas de información y se debe utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes así como perfiles de acceso a los sistemas, con el fin de evitar errores de integridad de la información utilizada en la entidad.
b. Se debe establecer ambientes separados para desarrollo, pruebas y producción (procesadores, dominios o directorios distintos), de manera que la funcionalidad de un ambiente no afecte al otro.
c. El ambiente de desarrollo y pruebas debe simular la configuración del ambiente de producción. Los datos que se manejen en este ambiente deben pasar por un proceso de enmascaramiento que permita asegurar la información.
d. La aprobación del pase de una aplicación o sistema de un ambiente a otro, se realizará de acuerdo a los procedimientos vigentes.

e. El acceso a los ambientes de desarrollo, pruebas y producción debe ser segregado.

12.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS [ISO 27001 A.12.2]

12.2.1. Controles contra códigos maliciosos [ISO 27001 A.12.2.1]

a. La INSI debe asegurar que todos los recursos informáticos estén protegidos mediante un software antivirus. Es responsabilidad del colaborador, del Área Encargada de la Atención a Usuarios de la INSI y de la Oficina de Seguridad Informática asegurar que el software antivirus no sea deshabilitado por ningún motivo.

b. Para prevenir eventos relacionados a códigos maliciosos, todos los colaboradores y personal de modalidades formativas de la SUNAT deben seguir los siguientes lineamientos:

- Esta prohibida la descarga, instalación y/o utilización de software no autorizado por la INSI, en los recursos informáticos provistos por la SUNAT.
- Esta prohibida la utilización de los recursos informáticos provistos por la SUNAT, para el ingreso a páginas web inseguras o que no estén relacionadas con las labores asignadas por la institución. Lo indicado se complementa con lo establecido en la Disposición Informática Administrativa de Uso del Servicio de Internet vigente, establecido por la INSI y de obligatorio cumplimiento.
- La INSI debe revisar periódicamente la instalación no autorizada de software en los equipos asignados a usuarios.
- En caso un usuario detecte código malicioso en un equipo provisto por la SUNAT, debe informar inmediatamente al área encargada de la atención a usuarios para que ejecuten el procedimiento vigente que corresponda para la atención de dichos casos.
- Se debe contar con las herramientas necesarias y actualizadas que permitan la detección y eliminación de código malicioso de manera automática.

- Se debe contar con procedimientos que permitan la recuperación ante una contingencia causada por código malicioso.

12.3. RESPALDO [ISO 27001 A.12.3]

12.3.1. Respaldo de la información [ISO 27001 A.12.3.1]

a. La INSI debe asegurar que toda la información almacenada en servidores y/o sistemas de almacenamiento sea resguardada mediante procedimientos manuales y/o automáticos que garanticen su identificación, protección y disponibilidad en caso que sea requerida.

b. Toda información resguardada en medios magnéticos 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 magnéticos u ópticos 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. La INSI debe establecer procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y períodos de retención de la misma.

e. El área encargada de operaciones y soporte a usuarios de la INSI debe establecer la existencia de sistemas manuales o automáticos de inventario de los medios magnéticos u ópticos que contengan la información resguardada. Estos sistemas deben permitir la identificación unívoca de los medios de almacenamiento, la identificación de la información contenida en ellos y la ubicación física

de los mismos para permitir un rápido y eficiente acceso a la información resguardada.

f. Todo nuevo servicio, base de datos, software, servidor y componente informático, debe tener su pase a producción, donde se debe especificar claramente los respaldos a realizar, así como la frecuencia y retención.

g. La SUNAT debe asegurar la tecnología adecuada para la realización de los respaldos institucionales, esto permitirá tener un estándar para la recuperación de la información ante alguna contingencia y adicionalmente migrar información histórica.

h. El respaldo de la información de la SUNAT, se debe realizar de acuerdo a lo establecido en el documento vigente de normas y pautas para la gestión de los respaldos y restauraciones informáticas.

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

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

a. Todos los sistemas de información de la SUNAT deben contar con la capacidad de registrar los eventos de seguridad y permitir el monitoreo de accesos indebidos e intrusiones. Todo sistema que maneje información importante de la SUNAT debe generar logs que almacenen información sobre actividades de los usuarios, activaciones y desactivaciones de los sistemas, excepciones, alarmas y eventos de seguridad de información, los cuales deben ser guardados durante un periodo definido para asistir futuras investigaciones y para el monitoreo de control de acceso.

b. La INSI 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 debe 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.

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

a. Los registros de auditoría deben protegerse contra su alteración y uso no autorizado según los lineamientos definidos en los documentos vigentes.
b. Las instalaciones y/o sistemas de almacenamiento de registros deben estar protegidas con mecanismos de acceso.
c. Se debe detectar cualquier modificación a los archivos de registro.
d. Se debe monitorear periódicamente la capacidad de almacenamiento para los registros.

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

a. Todas las actividades del administrador y operador del sistema deberán estar debidamente registradas y revisadas periódicamente por la Oficina de Seguridad Informática.
b. Para la generación y formato de los registros de auditoría deben seguirse los siguientes lineamientos:
    - Se debe registrar la actividad de los administradores y operadores del sistema, identificando a la persona, hora de ingreso, motivo del uso de la cuenta de acceso 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.

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

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

12.5. CONTROL DEL SOFTWARE OPERACIONAL [ISO 27001 A.12.5]

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

a. La INSI ha establecido los siguientes 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:
   - El pase a producción, configuración de cambios de los sistemas y código fuente, lo realizará personal autorizado de la INSI según lo especificado en los documentos vigentes.
   - Los sistemas deben presentar al usuario sólo código ejecutable y no código fuente.
   - Las pruebas para el pase a producción de un programa deben ser planeadas, ejecutadas, documentadas y controlados sus resultados, para garantizar la integridad de la información en producción. Estas pruebas deben realizarse en un ambiente distinto al de producción.
   - Se debe mantener un registro de todos los cambios realizados en el sistema.
   - Se deben almacenar las versiones de los sistemas anteriores a un cambio hasta que se compruebe que el cambio ha sido exitoso.

b. La instalación de software en sistemas operacionales debe realizarse según los lineamientos definidos en los documentos vigentes.

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

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

a. La Oficina de Seguridad Informática 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 sobre las vulnerabilidades técnicas de los sistemas utilizados que permita identificar los riesgos asociados y tomar acciones preventivas.

c. La INSI debe establecer un proceso de gestión de parches para que todo software operacional esté actualizado para asegurar los niveles óptimos de control y seguridad.
d. Los parches deben ser probados y evaluados antes de que sean instalados a fin de asegurar que sean efectivos y no causen efectos secundarios contraproducentes.
e. Se debe monitorear y evaluar la gestión de las vulnerabilidades técnicas para asegurar su efectividad y eficiencia por lo menos una vez por año.

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

a. Todo software para ser instalado y usado en cualquier equipo informático debe contar con la respectiva licencia o autorización de uso. En el caso de software libre de uso corporativo restringido, su utilización se efectúa de acuerdo a las restricciones establecidas en el informe de evaluación del área encargada de arquitectura (INSI).
b. El área encargada de la gestión de la infraestructura tecnológica debe llevar un registro de las licencias asignadas de software estándar adquirido por la SUNAT, así como de todo software estándar autorizado por el área encargada de la arquitectura (INSI).
c. El área encargada de la infraestructura tecnológica debe verificar que el software instalado en los servidores de la SUNAT cuente con el licenciamiento y/o autorización de uso. En caso contrario se procederá a la desinstalación del mismo.
d. El uso de software en la SUNAT debe hacerse de acuerdo a lo establecido en el documento vigente de políticas y normas para la utilización de software en la SUNAT.

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

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

a. Se deben realizar auditorías y revision de los controles de seguridad por lo menos una vez al año, dentro del plan de auditoría interna, a efectos de optimizar la efectividad de dichos controles. Estas auditorías deben contemplar la plataforma tecnológica y los procesos de gestión de la seguridad de la información de la SUNAT.
b. Toda actividad de auditoría debe estar planificada y acordada con el Oficial de Seguridad de la Información, previo a su ejecución, de modo que no afecte a la operatividad diaria evitando interrupciones graves en la plataforma tecnológica.
c. Para la ejecución de estas auditorías, toda la información necesaria debe estar limitada y disponible para los auditores con permiso de solo lectura.

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

13.1. GESTIÓN DE SEGURIDAD DE LA RED [ISO 27001 A.13.1]

13.1.1. Controles de la red [ISO 27001 A.13.1.1]

a. La INSI debe establecer un conjunto de controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de garantizar el buen uso de los mismos y mantener los niveles de seguridad establecidos de acuerdo a los resultados del análisis de riesgos sobre los activos de información.
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 de la SUNAT.
c. El acceso y uso del servicio de internet se debe realizar de acuerdo a lo establecido en el documento vigente de políticas y normas para el servicio internet en la SUNAT.
d. Los controles de redes deben realizarse según los siguientes lineamientos:
    - Para la conexión de sedes y equipos remotos, se deben utilizar conexiones seguras, privadas, dedicadas y/o encriptadas.
    - Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo de la empresa deben ser restringidas.

- Las conexiones de los equipos de cómputo y comunicaciones de la SUNAT deben realizarse sólo por personal autorizado.
- La red debe contar con mecanismos de detección de intrusos y contra la intercepción de información.
- Se debe garantizar una correcta segmentación de la red.

13.1.2. Seguridad de servicios de red [ISO 27001 A.13.1.2]

a. Se debe establecer que todos los sistemas y servicios de red estén actualizados con los parches y recomendaciones de los fabricantes para asegurar los niveles óptimos de control y seguridad.
b. La administración de las cuentas de acceso a internet, correo electrónico y otros servicios de red, debe ser realizada por el área encargada de la atención a usuarios de la SUNAT.
c. Cada Intendente, Gerente o Jefe de UUOO determina el acceso del personal a su cargo a los servicios de red, según amerite las funciones y actividades de cada colaborador.
d. Los servicios de red deben contar con mecanismos de detección y eliminación de código malicioso.
e. Se debe asignar una capacidad de almacenamiento fija para cada cuenta de correo electrónico, lo cual podrá variar de acuerdo al rol, funciones, cargo desempeñado o naturaleza de los buzones.
f. Los accesos a la red, internos y externos, deben contar con mecanismos de seguridad perimetrales.

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

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

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

13.2.1. Políticas y procedimientos de transferencia de la información [ISO 27001 A.13.2.1]

a. La SUNAT ha definido la presente Política de Transferencia de Información:
    - Toda la información en formato impreso o electrónico que sea utilizada entre la SUNAT y organizaciones o terceros vinculados con la institución, deberá estar sujeta bajo normativas de un Acuerdo de Confidencialidad Mutuo donde quedarán especificadas las responsabilidades para cada una de las partes.
    - La información intercambiada debe ser entregada al destinatario siguiendo los lineamientos de seguridad establecidos.
    - Toda información enviada a través del correo electrónico institucional, debe incluir un mensaje sobre su correcto uso, quedando bajo responsabilidad del receptor el cuidado y resguardo de la información.
    - El intercambio de información entre la SUNAT y un tercero se debe realizar según el procedimiento establecido entre la SUNAT y dicho tercero antes del inicio del intercambio.
    - Se debe contar con mecanismos para la detección y protección contra código malicioso que se puede encontrar en la información transmitida de forma electrónica.
    - Se debe contar con mecanismos para proteger la información transmitida de intercepción, copiado, modificación, cambio de ruta y destrucción.

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

a. Todos los medios de información con datos pertenecientes a la SUNAT que deban ser trasladados fuera de la entidad o ingresados desde algún lugar hacia la entidad, deben seguir los siguientes lineamientos:
    - Todo intercambio con terceros de información clasificada como restringida, confidencial o que afecte el principio de seguridad (confidencialidad), deberá realizarse tomando en cuenta los

riesgos que ello implica y sobre la base de acuerdos formales y estándares de intercambio.

- Debe notificarse el envío, despacho y/o recepción de información, asegurando la trazabilidad.

b. Para el intercambio de información entre instituciones y notificaciones oficiales a los contribuyentes, se debe propender a la utilización del correo electrónico seguro, para lo cual la Oficina de Seguridad Informática podrá recomendar el uso de firma y certificados digitales y/u otros mecanismos y procedimientos de seguridad informática y verificación adecuados.

13.2.3. Mensajes electrónicos [ISO 27001 A.13.2.3]

a. La INSI es responsable de la creación de una cultura y métodos, dentro de la entidad, acerca del buen uso del correo electrónico institucional.
b. Todo usuario es responsable por el contenido de todas las comunicaciones que almacene o envíe utilizando su cuenta de correo electrónico institucional.
c. Los usuarios autorizados no deben enviar mensajes de correo electrónico al exterior de la entidad, que hagan que ésta resultara dañada o agredida.
d. Se deben utilizar diversas técnicas para prevenir el correo spam.
e. Se deben implementar mecanismos para el bloqueo del ingreso y salida de mensajería no autorizada a la red de la SUNAT.
f. Los servicios de mensajería electrónica deben cumplir con las regulaciones legales vigentes.
g. Se debe asegurar el emisor, la dirección y transporte correcto del mensaje de la red interna de la SUNAT.
h. Debe utilizarse el servicio de correo electrónico que brinde la Institución para toda comunicación e intercambio de información que se transmita a través de este medio.
i. La gestión y uso del correo electrónico se debe realizar de acuerdo a lo establecido en el documento vigente políticas y normas para el correo electrónico institucional de la SUNAT.

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

a. Para todo tipo de contratación (a plazo fijo o indeterminado) se debe asegurar que el nuevo colaborador firme un acuerdo de confidencialidad para proteger los activos de información que este maneje. Con respecto a los terceros que contraten con la SUNAT, se deberán establecer acuerdos de servicios de carácter preventivo para que exista una previsión sobre la calidad del servicio recibido además de firmar un convenio de confidencialidad.
b. El personal de la SUNAT contratado por cualquier modalidad de contrato o modalidad formativa y los terceros vinculados deben firmar acuerdos o cláusulas donde se tipifique la confidencialidad de la información a la que tiene acceso como consecuencia del desempeño de sus funciones o de su desenvolvimiento dentro de la organización.
c. La vigencia de esta obligación de confidencialidad, se extiende incluso hasta después del cese de la relación contractual o laboral con la entidad.

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

14.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN [ISO 27001 A.14.1]

14.1.1. Análisis y especificación de requisitos de seguridad de la información [ISO 27001 A.14.1.1]

a. Siempre que se establezca un requerimiento nuevo para un sistema, se deben especificar los controles o requerimientos de seguridad asociados a él y a su implantación, además del análisis de riesgo y de impacto derivado en una posible falla.
b. El análisis y especificaciones de los requisitos de seguridad de la información para sistemas de información (adquiridos o desarrollados internamente), debe considerar lo siguiente:
    - El lenguaje a ser utilizado debe estar vigente y el soporte actualizado.

- Los controles para el ingreso y actualización de la información.
- Control de accesos.
- Registros de auditoría.
- Rutinas que se deben tomar en cuenta.
- Pautas para las pantallas y reportes.
- Separación de ambientes de desarrollo, pruebas y producción.

14.1.2. Aseguramiento de servicios de aplicaciones sobre redes públicas [SIO 27001 A.14.1.2]

a. Se debe realizar evaluaciones de riesgos y seleccionar los controles adecuados para proteger la información involucrada en los servicios de aplicación que pasan a través de redes públicas.
b. Para asegurar los servicios de aplicaciones en redes públicas se deben seguir los lineamientos especificados en los documentos vigentes.

14.1.3. Protección de transacciones en servicios de aplicación [ISO 27001 A.14.1.3]

a. Se deben adoptar controles de seguridad para transacciones en línea. El grado de dichos controles debe ser proporcional con el nivel del riesgo asociado con cada tipo de transacción en línea.
b. Las consideraciones de seguridad para transacciones en línea debe incluir lo siguiente:
    - Emplear firmas electrónicas por cada una de las partes implicadas en la transacción.
    - Todos los aspectos de la transacción.
    - Asegurar que la información confidencial de autenticación de todas las partes sean válidas y verificadas.
    - Asegurar que la transacción sea confidencial.
    - Asegurar la privacidad asociada a todas las partes implicadas.
    - Cifrar el canal de comunicación entre todas las partes implicadas.
    - Utilizar un protocolo seguro de comunicación entre todas las partes implicadas.

- Almacenar los detalles de la transacción fuera de cualquier ambiente público accesible.
- Cuando se emplea una autoridad confiable, la seguridad se integra e incorpora a través de todo el proceso completo de gestión del certificado/firma.

14.2. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE [ISO 27001 A.14.2]

14.2.1. Política de desarrollo seguro [ISO 27001 A.14.2.1]

a. Para el software desarrollado por personal de la entidad o adquirido a terceros se ha definido la presente Política de Desarrollo de Seguridad:
   - Se debe establecer la seguridad del entorno de desarrollo.
   - Se debe establecer la seguridad en la metodología de desarrollo de software (ciclo de vida del desarrollo de software).
   - Se deben fijar las directrices de codificación para cada lenguaje de programación utilizado.
   - Se deben establecer los requisitos de seguridad en la etapa de diseño.
   - Se deben establecer los controles de seguridad dentro de los hitos del proyecto.
   - Se deben contemplar los registros de seguridad.
   - Se debe establecer la seguridad en el control de la versión.
   - Se debe elaborar, mantener y aplicar un procedimiento para la incorporación de sistemas de información, el cual debe incluir lineamientos, procesos, buenas prácticas, plantillas y guías que sirvan para regular los desarrollos de productos de software internos en un ambiente de aseguramiento de calidad.

14.2.2. Procedimientos de control de cambio del sistema [ISO 27001 A.14.2.2]

a. Todo sistema y aplicaciones utilizados para el procesamiento de la información de la SUNAT debe ser instalado y actualizado a través de

procedimientos formales de control de cambios los cuales deben asegurar que sólo los cambios autorizados sean implantados. Deben existir procedimientos que obliguen a una aprobación formal por parte de las áreas propietarias de la información, para que los programas sean implantados en los entornos de producción. Debe mantenerse un registro de todas las implantaciones realizadas en el ambiente de producción y para identificar quién, cuándo y dónde se realizó la instalación.

b. El control de cambios debe seguir los lineamientos definidos en los documentos vigentes. Entre ellos:
    - Registro de todos los accesos y cambios.
    - Revisión de mantenimiento de la integridad de la información.
    - Aceptación de los cambios por parte del usuario.
    - Actualización de la documentación del sistema.
    - Control de versiones.
    - Se debe asegurar que los cambios a aplicar no comprometan los controles de seguridad de información ya implementados.
    - Los cambios deben ser planificados para no afectar la operatividad del sistema.

14.2.3. Revisión técnica de aplicaciones después de cambios a la plataforma operativa [ISO 27001 A.14.2.3]

a. Se debe revisar y probar los módulos o programas que han sido materia de cambios, para asegurar que no afectan al funcionamiento o seguridad del sistema operativo.

b. Se debe garantizar la asignación de recursos para revisiones, mantenimientos, pruebas y cambios en el sistema operativo. Cuando se realicen cambios o actualizaciones a los sistemas operativos, se deben realizar pruebas para garantizar que no se afecta la seguridad de los mismos.

14.2.4. Restricciones sobre cambios a los paquetes de software [ISO 27001 A.14.2.4]

a. Se debe limitar a los necesarios los cambios a los paquetes de software proporcionados por terceros, de manera que no debilite su estructura y no genere un gran impacto para la entidad por el mantenimiento de dicho software.
b. Se debe considerar en la planificación, la adquisición de las actualizaciones de software de terceros siempre que corresponda.
c. Las actualizaciones de software de terceros deben ser probadas antes de su pase a producción.

14.2.5. Principios de ingeniería de sistemas seguros [ISO 27001 A.14.2.5]

El desarrollo de software debe aplicar técnicas seguras de ingeniería, las cuales deben estar documentadas y deben revisarse periódicamente, para tal fin se debe cumplir con la documentación vigente que sea aplicable.

14.2.6. Ambiente de desarrollo seguro [ISO 27001 A.14.2.6]

Se debe contar con control de acceso físico y lógico al ambiente de desarrollo de software.

14.2.7. Desarrollo contratado externamente [ISO 27001 A.14.2.7]

a. El desarrollo de software por terceros debe cumplir con los lineamientos relacionados al desarrollo y mantenimiento de sistemas de información y todos los controles asociados.
b. Al recibir el sistema terminado, se deben realizar todas las pruebas bajo los mismos procedimientos establecidos para el desarrollo interno, a fin de certificar la calidad, seguridad y exactitud del trabajo realizado.
c. Se debe considerar en el contrato, acuerdos de licenciamiento, propiedad del código, derechos de propiedad intelectual y servicio de soporte y mantenimiento.
d. Debe realizarse estrictamente la supervisión de los contratos y seguimiento de las actividades de desarrollo de software desarrollado por terceros.

14.2.8. Pruebas de seguridad del sistema [ISO 27001 A.12.4.8]

Se deben realizar pruebas de las funcionalidades de seguridad, tanto para el software desarrollado internamente como el desarrollado por terceros.

14.2.9. Pruebas de aceptación del sistema [ISO 27001 A.12.4.9]

a. Para el caso de actualizaciones y cambios de versiones de los sistemas de procesamiento de información críticos, debe existir una autorización formal de aceptación por parte del propietario (responsable del sistema), luego de haber realizado las pruebas necesarias de funcionamiento apropiado.
b. Los cambios se deben regir por los lineamientos definidos en los documentos vigentes.

14.3. DATOS DE PRUEBA [ISO 27001 A.14.3]

14.3.1. Protección de datos de prueba [ISO 27001 A.14.3.1]

a. Las pruebas de aceptación se deben realizar en un ambiente de pruebas separado del ambiente de producción.
b. Los datos de producción no deben ser accedidos desde el ambiente de pruebas para la ejecución de las mismas.
c. Se debe proveer medidas adecuadas de seguridad para prevenir la exposición de datos de pruebas sensibles.
d. Se debe registrar la copia y uso de la información de pruebas.
e. Toda prueba de software que deba realizarse con datos de producción, no debe contener detalles específicos de los mismos que puedan ser críticos o sensibles. Se deben definir los procedimientos para el uso de la información requerida.
f. Los ambientes de prueba deben tener implementados los mismos mecanismos de seguridad y de control de acceso que los sistemas de producción.

15. RELACIONES CON LOS PROVEEDORES (ISO-A.15)

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

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

a. La SUNAT ha establecido la presente Política de Seguridad de Información para la relación con los proveedores:

- Los terceros deben firmar acuerdos de confidencialidad al momento del inicio de sus contratos, en los cuales se comprometen a no divulgar, usar o explotar la información de la entidad a la cual tengan acceso.
- En el caso de terceros con acceso a información de los sistemas de la SUNAT, debe ser responsabilidad de los Intendentes, Gerentes o Jefes de UUOO o la INA, según corresponda, informar oportunamente a la INSI sobre el fin de los contratos con terceros, para tomar las medidas preventivas y correctivas de acuerdo a sus procedimientos vigentes.
- La información institucional administrada, manejada o creada por terceros debe ser de la entidad al igual que los sistemas de información desarrollados por terceros; por lo anterior, la SUNAT debe ser propietaria de los derechos de esta información.
- Está prohibido realizar copias no autorizadas de software, debido a la Ley sobre el Derecho de Autor.
- No se debe proveer información sobre la ubicación de los Centros de Cómputo o de los lugares críticos, como mecanismo de seguridad.
- El servicio entregado por terceros según su criticidad e impacto en la continuidad del negocio, debe incluir parámetros de seguridad de información dentro del contrato establecido con la SUNAT o del Acuerdo de Nivel de Servicio (SLA – Service Level Agreement), de ser el caso y contemplar penalidades ante el incumplimiento.
- El nivel de servicio de los terceros (SLA) debe ser evaluado y aceptado por la INSI.

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

a. Los Usuarios del Servicio deben definir los requisitos de seguridad con terceros los cuales se deben incluir en los Contratos u Órdenes de Servicio y también términos de referencia debe incluirse en los Acuerdos de Confidencialidad con Terceros.
b. Se debe definir los requisitos de seguridad de la información para los servicios de tecnología de la información y comunicación, que incluya que los proveedores consideren estos requisitos de seguridad de la información, en toda la cadena de suministro.

15.2. GESTIÓN DE ENTREGA DE SERVICIOS DEL PROVEEDOR [ISO 27001 A.15.2]

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

a. Los servicios de terceros se deben monitorear y revisar de acuerdo a lo especificado en el Contrato u Orden de Servicio.
b. El monitoreo y revisión de los servicios de terceros se debe realizar siguiendo los lineamientos definidos. Entre ellos:
    - Se debe monitorear y revisar periódicamente los registros y reportes emitidos por los servicios de terceros, para verificar el cumplimiento de los parámetros de seguridad de información establecidos.
    - Las áreas deben comunicar las fallas e incidentes en los servicios de terceros según lo especificado en los documentos vigentes.

15.2.2. Gestión de cambios a los servicios de proveedores [ISO 27001 A.15.2.2]

a. Se debe mantener la operación de la SUNAT controlando el impacto de los servicios de terceros ante cambios.

b. Se debe registrar todos los cambios y mejoras realizados en los sistemas de comunicaciones u operaciones por servicios externos según los documentos vigentes.

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

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

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

Las actividades para la gestión de incidentes de seguridad de la información que aseguran una respuesta rápida, efectiva y ordenada a éstos, así como los roles y responsabilidades en la gestión, han sido definidas en el Manual de Roles, Responsabilidades y Autoridades Organizacionales del SGSI (SGSI-MA-02) y en el Procedimiento para el registro y atención de incidentes y vulnerabilidades de seguridad de la información vigentes.

16.1.2. Reporte de eventos de seguridad de la información [ISO 27001 A.16.1.2], Reporte de vulnerabilidades de seguridad de la información [ISO 27001 A.16.1.3]

a. Se debe realizar, en forma periódica, un análisis de vulnerabilidades, así como evaluaciones de riesgos sobre los activos de información según lo especificado en el documento Metodología de Gestión de Riesgos de Seguridad de la Información vigente.
b. Todos los colaboradores y personal de modalidades formativas de la SUNAT o terceros que, durante el desempeño de sus labores diarias, identifique una vulnerabilidad o sospeche de un evento que comprometa o pueda comprometer las operaciones y afectar la seguridad de la información de la institución, deben reportarlo inmediatamente a través de los canales de comunicación establecidos en el Procedimiento para el registro y atención de incidentes y vulnerabilidades de seguridad de la información vigente.
c. Los colaboradores y personal de modalidades formativas o terceros que generen un incidente de seguridad de información, de manera

intencional o accidental, será considerado como falta que podrá ser sancionada según los controles y procedimientos vigentes de la SUNAT.

d. Los sistemas de información deben contar con registros de eventos de seguridad y, en lo posible, generar alertas.
e. Ningún colaborador, ni personal de modalidades formativas de la SUNAT o tercero deben tratar de probar o explotar una vulnerabilidad sin autorización y como parte de un proceso controlado. Dicho incumplimiento será considerado como falta que podrá ser sancionada según los criterios y normativas de la SUNAT.

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

a. De acuerdo a lo definido en el Procedimiento para el registro y atención de incidentes de seguridad de la información vigente, 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.
b. Las alertas generadas automáticamente por herramientas de seguridad y/o monitoreo, deben servir como insumo del personal de las áreas de la INSI para el reporte de eventos y vulnerabilidades de seguridad de la información a través de los canales de comunicación establecidos en el Procedimiento para el registro y atención de incidentes de seguridad de la información vigente.
c. El personal de las unidades organizacionales que por función y/o coordinación intervienen en la atención de los incidentes y vulnerabilidades de seguridad de la información, deberán mantener la reserva y confidencialidad de los casos.

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

a. Los incidentes de seguridad de la información deben responderse de acuerdo a lo definido en el Procedimiento para el registro y atención

de incidentes de seguridad de la información vigente. Según sea el caso, se debe contemplar:

- Considerar para la solución de un incidente, realizar el análisis de causa raíz, la definición de acciones correctivas y preventivas, reportes a la jefatura, entre otros.
- Cuando sea necesario, se deberá guardar evidencia del incidente, para poder investigar las causas del mismo.
- Todas las medidas correctivas y acciones de emergencia deben ser ejecutadas sólo por personal autorizado.
- Se debe mantener los contactos actualizados según su nivel de escalamiento al interno o con servicios dados por terceros.

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

Se deben registrar los incidentes ocurridos, tipos, causas, el impacto ocasionado y forma de resolución, con el objeto de tener estadísticas anuales de comportamiento de respuesta ante incidentes, aprender de lo ocurrido y establecer mejoras en las acciones de control y las políticas de seguridad de la información cuando sea necesario; lo cual deberá realizarse según lo definido en el Procedimiento para el registro y atención de incidentes de seguridad de la información vigente.

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

a. El personal de las unidades organizacionales que por función y/o coordinación intervienen en la atención de los incidentes y vulnerabilidades de seguridad de la información deben mantener las evidencias de las actividades ejecutadas considerando lo definido en el Procedimiento para el registro y atención de incidentes de seguridad de la información vigente.
b. Cuando una acción de seguimiento contra una persona u organización, después de un incidente de seguridad de la información, implique acción legal, la evidencia debe ser recolectada, retenida y presentada para estar conforme con las reglas para la

colocación de evidencia en la jurisdicción relevante. Para ello los sistemas críticos deben cumplir con cualquier estándar o código para la producción de evidencia admisible.

c. Se debe implementar controles de acceso y protección para dicha evidencia.

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

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

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

La SUNAT debe asegurar la continuidad de las operaciones en caso de una contingencia no prevista con el fin de reducir el impacto en el negocio. Para ello debe existir un plan de contingencia debidamente documentado y administrado “en sitio” para el desarrollo y mantenimiento de los servicios informáticos de la SUNAT denominado Plan de Recuperación de Desastres; el cual debe estar elaborado en base a los lineamientos y requerimientos de la seguridad de la información y debe estar sujeto a escalamiento y pruebas.

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

a. La SUNAT debe contar con procedimientos que permitan 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 vigente del Plan de Recuperación de Desastres.

17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información [ISO 27001 A.17.1.3]

a. El Plan de Recuperación de Desastres debe ser revisado periódicamente para que se encuentre actualizado al momento de ser

probado y se encuentre alineado a la realidad de las operaciones en la entidad.

b. Periódicamente se debe probar la efectividad del Plan de Recuperación de Desastres 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.

17.2. REDUNDANCIAS [ISO 27001 A.17.2]

17.2.1. Instalaciones de procesamiento de la información [ISO 27001 A.17.2.1]

La SUNAT debe implementar las instalaciones de procesamiento de información con redundancia suficiente para cumplir con el requisito de disponibilidad.

18. CUMPLIMIENTO (ISO 27001-A.18)

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

18.1.1. Identificación de requisitos contractuales y de legislación aplicables [ISO 27001 A.18.1.1]

a. La SUNAT debe establecer que ante cualquier requerimiento legal que esté relacionado con los sistemas informáticos o los usuarios internos, se observarán las leyes vigentes mediante el asesoramiento legal respectivo para asegurar los requisitos regulatorios que apliquen.

b. Se debe identificar, documentar, mantener y cumplir todos los requisitos legales, regulatorios y contractuales para los sistemas de información de la SUNAT.

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

a. Se debe tener un control respecto de la cantidad y vigencia de las licencias de software base (sistemas operativos), base de datos y aplicaciones comerciales utilizadas por la SUNAT. El incumplimiento de este control puede traducirse en la utilización de software adquirido en forma ilegal que comprometa la imagen y perjudique, económica

o legalmente, a la entidad. Adicionalmente, los contratos con terceros deben contemplar aspectos referidos a los derechos de propiedad intelectual.

b. Se deben archivar todas las licencias de software base (sistemas operativos), base de datos y aplicaciones comerciales adquiridas, a fin de que se encuentren disponibles en caso que sean requeridas por auditoría legal.
c. Se debe revisar en forma periódica los sistemas de información y estaciones de trabajo/laptops, a fin de verificar la no existencia de copias de software no licenciado. El usuario será responsable por el contenido de programas no autorizados en el disco duro de dichos equipos.
d. Se debe contar con cláusulas de cumplimiento de restricciones legales, reguladoras y contractuales sobre el uso de material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario, especificados en los contratos con terceros.

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

Se deben establecer los lineamientos que aseguren la protección de los registros contra pérdida, destrucción, falsificación y acceso no autorizado, en concordancia con los requisitos legales, regulatorios y contractuales, lo cual se debe realizar según los lineamientos definidos en los documentos vigentes.

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

a. Se debe contar con cláusulas de privacidad y de protección de datos personales en los contratos con terceros, de acuerdo con la Ley N° 29733 Ley de Protección de Datos Personales, la cual es de obligatorio cumplimiento.
b. Los registros de personal y sus datos privados deben protegerse y almacenarse en lugar seguro para evitar robo de información privada que pueda afectar la integridad del personal de la SUNAT, lo cual se

debe realizar según los lineamientos definidos en los documentos vigentes.

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

Los controles criptográficos deben ser establecidos y utilizados en conformidad con todos los acuerdos, leyes y regulaciones vigentes.

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

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

a. El Oficial de Seguridad de la Información debe asegurarse que se realicen revisiones periódicas de seguridad por auditores independientes del área bajo revisión.
b. Las auditorías al SGSI deben realizarse de acuerdo a los lineamientos definidos en el Procedimiento de Auditoría Interna (SGSI-PR-05).

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

a. El Oficial de Seguridad de la Información en conjunto con el CGD deben asegurar que todas las políticas, procedimientos y estándares de seguridad de la información definidos por la SUNAT son cumplidas en su totalidad.
b. Los Intendentes, Gerentes o Jefes de UUOO deben asegurarse que se cumplan correctamente todos las políticas y procedimientos de seguridad de información, al ser los gestores directos en su área de responsabilidad. Asimismo, deben informar oportunamente al Oficial de Seguridad de la Información en caso de su incumplimiento.
c. Cualquier inquietud o duda que generase la aplicación o interpretación de estas políticas debe ser consultada necesariamente al Oficial de Seguridad de la Información.

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

Todos los sistemas informáticos de la SUNAT deben ser verificados periódicamente para asegurar el cumplimiento de los niveles

apropiados de seguridad. La INSI debe comprobar la conformidad técnica de los sistemas de información con las normas de seguridad de información, ya sea manual o automáticamente.

19. CONTROL DE CAMBIOS

Detalle	Versión	Fecha de Aprobación	Responsable
Versión inicial del documento	01	04/02/2019	Oficial de Seguridad de la Información
Actualización integral del documento	02	22/03/2023	Oficial de Seguridad de la Información