LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD DE LA INFORMACIÓN

ROL	NOMBRE	PUESTO/ROL
Modificado por:	Luis Víctor Méndez Montoya	Oficial de Seguridad y Confianza Digital
Revisado por:	Kelly Elizabeth Paz Orellana	Jefa (e) de la Unidad de Modernización
	José Antonio Callirgos Paz	Jefe de la Oficina de Tecnologías de Información
Aprobado por:	Manuel Fernando Muñoz Quiroz	Gerente General

CONTROL DE CAMBIOS

N°	Ítems (Sección del documento)	Descripción del cambio (*)
1	5. DEFINICIONES	• Se modificó la definición de “Software malicioso (malware)” para precisarla.
2	7.2 DISPOSITIVOS MOVILES,	• Se modificó el orden de los numerales para estructurar el contenido en disposiciones generales, de responsabilidad de la OTI y por último las que son de responsabilidad del usuario. • En el numeral 7.2.1 - Se eliminó la frase “Los dispositivos móviles del tipo smartphone, son asignados a los/as usuarios/as por la OTI mediante la firma de una ficha de asignación de equipos”, con el fin de aclarar que la OTI no se encarga de la asignación de dichos dispositivos. • En el numeral 7.2.2 (antes 7.2.4) - Se modificó su redacción para precisar que en general todos los dispositivos móviles deben contar con mecanismos de autenticación y se eliminó la frase redundante "que almacenan o guarden información", ya que es implícito que los dispositivos móviles almacenan información. Asimismo, se eliminó la oración “Las capacidades del dispositivo móvil, respecto del control de acceso, son definidas en función de la importancia de la información que se almacena o se protege en cada dispositivo móvil”, ya que esta información no es relevante para el mensaje principal. • En el numeral 7.2.3 (antes 7.2.5) - Se modificó para precisar que los dispositivos móviles deben contar con la última versión o la más segura de los sistemas operativos; así como, de los parches y aplicaciones provenientes del fabricante. Esta medida resulta fundamental para minimizar las vulnerabilidades y proteger la información almacenada en dichos dispositivos. • Se agregó el numeral 7.2.5. • En el numeral 7.2.6 - En el literal a), antes numeral 7.2.2, se eliminó la frase “los dispositivos móviles de” y se modificó su redacción para precisar la responsabilidad de manera clara y concisa. - Se agregaron las responsabilidades de los literales b), c), d), e) y f). • En el numeral 7.2.7 - En el literal a), antes primer párrafo del numeral 7.2.6, se eliminó la frase “El/la usuario/a es responsable” ya que esta información se encuentra establecida al inicio del numeral. - En el primer punto del literal b), antes numeral 7.2.3, se modificó la redacción precisando que la solicitud de migración de información a un nuevo dispositivo móvil es responsabilidad del usuario. - En el segundo punto del literal b), antes numeral 7.2.7, se modificó la redacción precisando que el smartphone asignado no debe ser entregado a otra persona. - Se agregaron las responsabilidades de los literales c), d), e) y f). - En el literal g), antes literal “a” del numeral 7.2.9, se agregó la oración “El usuario es responsable de toda actividad realizada en el dispositivo móvil asignado”. • En el numeral 7.2.8 (antes literal b) del numeral 7.2.9) - Se agregó la frase “En caso de pérdida o robo, el usuario en un máximo de 24 horas debe realizar la denuncia policial respectiva” para precisar el tiempo máximo en el que se deber realizar la denuncia. - Se agregó el segundo párrafo para precisar que la OTI es responsable de activar el restablecimiento remoto del equipo.

N°	Ítems (Sección del documento)	Descripción del cambio (*)
3	7.3 TELETRABAJO	• Se agregó un párrafo antes del numeral 7.3.1 para precisar que todo el personal que realiza teletrabajo parcial o total debe firmar la "Declaración Jurada sobre el Uso de Recursos, Servicios Informáticos, Confianza Digital, Protección y Confidencialidad de los Datos de la Sunass bajo la Modalidad de Teletrabajo" entregada por la URH." Porque en este documento se han establecido lineamientos que se deben cumplir con relación al uso de los sistemas de información y equipos informáticos asignados por la Sunass; asi como tambien, para aquellos casos en el que se emplean equipos informáticos personales para el desempeño de sus funciones. • Se modificó las viñetas a numeración con vocales en todos los numerales para facilitar la descripción del control de cambios. • En el numeral 7.3.1 - En los 3 últimos puntos del literal a), se agregaron las responsabilidades que el personal debe cumplir para garantizar la privacidad y protección de la información que es de su manejo.: - En el literal c), se agregó las siguientes frases o "Garantizar que todos los trabajos realizados en la modalidad de teletrabajo se guarden en la plataforma tecnológica de la SUNASS" para precisar que es responsabilidad del guardar dicha información en la ubicación de almacenamiento señalada por la OTI. o "Mis documentos" • En el numeral 7.3.2 - En el literal e), se reemplazó el texto "AnyDesk" por la frase "y la solución de administración remota autorizada por la OTI para el soporte al usuario". - Se eliminó la responsabilidad "Anular los accesos a los sistemas de información cuando finalicen las actividades remotas". - Se reemplazó el literal f)para precisar la necesidad de verificar la seguridad de las herramientas utilizadas por el personal de soporte de la OTI, para el acceso remoto a los equipos del personal en modalidad de teletrabajo. - Se agregaron las responsabilidades de los literales h) e i).
4	7.5 GESTIÓN DE ACTIVOS	• En el numeral 7.5.2 - En los 6 últimos puntos del literal c), se agregaron las responsabilidades que debe cumplir la OTI respecto al manejo de los activos de información. • En el numeral 7.5.3 - Se eliminó el primer punto de este numeral "Debe identificarse los elementos que puedan requerir su eliminación". - Se agregaron las disposiciones de los literales a), b) e i) para el manejo de los medios removibles. - En el literal e), se reemplazó el texto "tengan" por "disponga de" para precisarlo. - Se agregó la oración "el borrado seguro también se aplica en el caso que el medio removible sea reutilizado por otro personal".
5	7.6 CONTROL DE ACCESO	• Se reemplazó el texto "y a los servicios de red" con "y/o recursos informáticos". • Se agregó el numeral 7.6.1 para precisar el alcance de la aplicación de los requisitos descritos para el control de acceso. • En el numeral 7.6.2 (antes 7.6.1): - En el literal a), se eliminó el primer aspecto a tener en cuenta para el acceso a los activos de información: La coherencia entre los lineamientos de control de acceso y de gestión de activos de información. - En el primer punto del literal a), se eliminó el texto "estandarizados" y se reemplazó el texto "roles" por "necesidad y siguiendo el principio de mínimo privilegio".

N°	Ítems (Sección del documento)	Descripción del cambio (*)
		- En el segundo punto del literal a), se agregó el texto "por parte del equipo de seguridad informática". - En el literal c), se reemplazó el texto "la red y servicios de red " por "los servicios de red " y "responsable de la unidad de organización" por "responsable designado de la unidad". - Se elimino la disposición "El acceso a los recursos de red debe ser controlado, de manera que el personal no comprometa la seguridad de los activos de información", antes literal d). - Se agregaron las disposiciones de los literales d) y e). • En el numeral 7.6.3 (antes 7.6.2): - Se agregó el literal d) - Se modificó la redacción del literal e) para precisar que la contraseña debe contener como mínimo un carácter en mayúscula, minúscula, un número y un carácter especial. • En el numeral 7.6.4 (antes 7.6.3): - Se modificó la redacción del literal b) para precisar que la creación de los usuarios genéricos no requiere de la autorización del Oficial de Seguridad y Confianza Digital. - En el literal f), se agregó el texto "en el servidor de archivos" para precisar la ubicación de la carpeta compartida. - En el literal g) se agregó el texto "o a quien designe" para precisar que la información de la baja de usuarios no sólo la puede informar el/la Jefe/a de la URH. - En el literal h), se eliminó el texto "como aquellos que no gestiona" por ser redundante. - Se reformularon todas las disposiciones del literal i). - Se modificó la redacción del literal j), para precisar que las credenciales de acceso son enviadas directamente al usuario y que por seguridad está obligado a cambiar su contraseña al acceder por primera vez. - Se modificó la redacción del literal k) para precisar que cada seis meses se realiza una revisión de los accesos de todos los usuarios y de identificar algún usuario que no debe tener acceso o si se requiere efectuar alguna actualización se debe contar con la validación del responsable de la unidad de organización Se modificó la redacción del literal l) para precisar que la información y la cuenta del usuario es almacenada por un periodo mínimo de tres meses y luego se elimina. Asimismo, se agregó la oración "Todas las excepciones a esta regla deberán ser comunicadas al Oficial de Seguridad y Confianza Digital" para señalar que pueden existir excepciones. - Se agrego la disposición del literal m). • En numeral 7.6.5 (antes 7.6.4): - En el literal b), se reemplazó el texto "con lo configurado en el Active Directory" por "a lo estipulado con el presente lineamiento". - Se agregaron las disposiciones de los literales f), g), h) e i). • En el numeral 7.6.5 se cambió por el numeral 7.6.6 - En el literal a), se eliminó el texto "también los datos y aplicaciones por el usuario". - En el literal c), se reemplazó la frase "está restringido y se limita el uso sólo para usuarios/as autorizados/as y debe ser también controlado" por "que vulneren los controles de seguridad, no debe ser instalados ni utilizados bajo sanción como se estipula en el RISS". - En el literal d), se reemplazó la frase "definición y documentación" por "en el inventario de software autorizado por el Especialista en Arquitectura y Soluciones TI". - En el literal e), se precisó que la Mesa de Ayuda de la OTI es responsable de desactivar y/o eliminar todo programa que no se encuentre en el inventario de software autorizado. - Se agregaron las disposiciones de los literales g) y h).
6	7.7 CRIPTOGRAFÍA	• Se complementó la disposición al precisar que se debe emplear un listado de software No autorizado para evitar su uso o un listado de software autorizado.

N°	Ítems (Sección del documento)	Descripción del cambio (*)
8	7.10 SEGURIDAD DE LAS OPERACIONES	• En el numeral 7.10.3: - Se agregó la disposición del literal a). • En el numeral 7.10.4: - Se modificó la redacción del literal a) y d). - Se agregaron las disposiciones de los literales e) y f). • En el numeral 7.10.5: - Se agregó la disposición del literal f). • En el numeral 7.10.6: - En el literal a), se reemplazó el texto “antivirus” por “protección de códigos maliciosos”. - En el literal b) y c), se reemplazó el texto “antivirus” por “protección de códigos maliciosos”. - En el literal d), se agregó el correo electrónico de la Mesa de Ayuda de la OTI. - Se agregaron las disposiciones de los literales e) y f). • En el numeral 7.10.9: - Se agregaron las disposiciones de los literales a), b) y d). : • En el numeral 7.10.10 - Se eliminó la disposición “La OTI debe asegurar que el software que se va a instalar se encuentre identificado en la lista de softwares permitidos.” - Se agregó la disposición del literal f). • En el numeral 7.10.11: - Se agregaron las disposiciones de los literales d) y e).
9	7.11 SEGURIDAD DE LAS COMUNICACIONES	• En el numeral 7.11.1 - Se agregaron las disposiciones de los literales d), j) y k). - En el literal e), se eliminó el texto “frecuentemente” para no establecer un periodo de revisión. - Se eliminó la disposición “Se cuenta con el Active Directory instalado en el servidor interno para separar los archivos compartidos entre los usuarios”. . • En el numeral 7.11.2: - En el literal a), se reemplazó el texto “antivirus actualizado” por “sistema de protección de código malicioso” y “software malicioso” por el texto “virus, malware, entre otros.” - En el literal b), se eliminó el texto “estos deben realizarse utilizando el protocolo HTTPS, FTP y una clave que se le asignará previa petición” y “en caso de no existir, se le debe de hacer firmar uno”. - Se agregaron las disposiciones de los literales c), f), h) e i).
10	7.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	• En el numeral 7.12.2: - En el literal e), se eliminó el texto “Desarrollo seguro para el diseño y codificación (elaboración de código seguro)”. - En el literal g), se reemplazó el texto “subcontratados” por “contratados como terceros”. • Se agregaron las disposiciones del numeral 7.12.4.
11	7.13 DESARROLLO SEGURO	• En el literal b), se agregó el texto “aplicable al proyecto de desarrollo” para complementarlo. • Se agregaron las disposiciones de los literales c), e), f), g), h), i), j), l), m) y n). • En el literal p),se eliminaron los siguientes requisitos: - Los/as usuarios/as deben estar sincronizados para sistemas web con el Active Directory administrado por la OTI.

N°	Ítems (Sección del documento)	Descripción del cambio (*)
		- Otras que la OTI solicite. • Se eliminaron las siguientes disposiciones: - Los requerimientos se analizan y validan para asegurar que son necesarios, balanceando restricciones rente a necesidades y asegurando que el producto funcionará en el ambiente de producción. - El diseño del producto debe incluir el diseño de las interfaces y un análisis de lo que debe desarrollarse, comprarse o reusarse. Los manuales deben incluir la documentación de uso final que brinde soporte al mismo. - La integración de los componentes del producto se debe realizar definiendo y siguiendo un procedimiento establecido. Las compatibilidades de las interfaces deben ser aseguradas y el producto integrado evaluado antes de su entrega. - Para asegurar los requerimientos especificados se realiza la verificación, lo cual implica la selección de productos, el establecimiento del ambiente donde el producto será verificado y realizar la verificación siguiendo procedimientos y criterios establecidos, los resultados deben ser analizados. - Se utilizan técnicas de programación segura para los desarrollos: Las aplicaciones exigen a los/as usuarios/as que utilicen contraseñas seguras y Reutilizar componentes de confianza.
12	7.14 SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES	• Se agregaron las disposiciones de los numerales 7.14.3, 7.14.10, 7.14.11, 7.14.12, 7.14.13, 7.14.14 y 7.14.15.

(*) Los cambios señalados son respecto a la versión anterior.

ÍNDICE

1. OBJETIVO

Establecer los lineamientos de seguridad de la información en la SUNASS, a fin de proteger la confidencialidad, disponibilidad e integridad de la información, recursos, servicios e instalaciones de la entidad. Los lineamientos se encuentran alineados a la Política del SIG y al contexto de la gestión de riesgos de seguridad de la información, el cual brinda el marco para el establecimiento de los controles de seguridad de la información.

2. ALCANCE

El presente documento aplica a todo el personal y las partes interesadas que forman parte de la gestión de la seguridad de la información de la SUNASS.

3. BASE NORMATIVA

3.1 Ley Nº 27658, Ley Marco de modernización de la Gestión del Estado.
3.2 Decreto Supremo Nº 103-2022-PCM, Política Nacional de Modernización de la Gestión Pública al 2030.
3.3 Decreto Supremo Nº 123-2018-PCM, Reglamento del Sistema Administrativo de Modernización de la Gestión Pública.
3.4 Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001 :2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
3.5 Norma Técnica Peruana NTP – ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Seguridad de la Información. Requisitos.
3.6 Norma Técnica Peruana NTP – ISO/IEC 27002:2017 "Tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información.
3.7 Ley N° 29733 "Protección de Datos Personales, sus modificatorias y Reglamento". Decreto Legislativo N.º 1353, Autoridad Nacional de Transparencia y Acceso a la Información Pública, Fortalece el Régimen de Protección de Datos Personales y la Regulación de Gestión de Intereses.
3.8 Decreto Supremo Nº 029-2021-PCM, aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
3.9 Decreto Supremo Nº 157-2021-PCM, aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

4. SIGLAS / ACRONIMOS

OAJ : Oficina de Asesoría Jurídica
OTI : Oficina de Tecnologías de la Información
RISS : Reglamento Interno de Servidores Civiles de la Sunass.
SIG : Sistema Integrado de Gestión.
SIG : Sistema Integrado de Gestión.
SGSI : Sistema de Gestión de Seguridad de la Información
TIC : Tecnologías de la Información y la Comunicación
URH : Unidad de Recursos Humanos
UA : Unidad de Abastecimiento

5. DEFINICIONES

5.1 **Acceso remoto:** Es el acceso realizado desde un equipo informático a un recurso ubicado físicamente en otra computadora que se encuentra en otro lugar.

5.2 Activos de Información: Es el bien o servicio tangible o intangible, que genera, procesa o almacena información, en el cual se le atribuye un grado de valor según su criticidad o asociación con los procesos misionales.

5.3 Cifrado: Es el mensaje escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave necesaria para descifrarlos.

5.4 Contraseña: Es una cadena de caracteres que se puede usar para iniciar sesión en un equipo y obtener acceso a archivos, programas y otros recursos.

5.5 Copia de respaldo (backup): Es la copia de los datos de un archivo automatizado en un soporte que posibilite su recuperación.

5.6 Correo electrónico: Es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes o cartas electrónicos) mediante sistemas de comunicación electrónicos.

5.7 Criptografía: Son técnicas de cifrado destinadas a alterar las representaciones lingüísticas de ciertos mensajes con el fin de hacerlos ininteligibles a receptores no autorizados.

5.8 Dispositivo móvil: Son los dispositivos que permiten acceder a datos e información desde cualquier lugar y en cualquier momento. Comprenden las Laptops, Smartphones, iPad y Tablets.

5.9 Medio removible: Es cualquier componente extraíble de hardware, usado para el almacenamiento de información. Por ejemplo, cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

5.10 Propietario de activo de información: Es la persona que tiene la responsabilidad de controlar la producción, desarrollo, mantenimiento, uso y seguridad de un activo de información. El término “propietario” no significa que la persona tenga en realidad derechos de propiedad sobre el activo.

5.11 Proveedor: Es la persona natural o jurídica que brinda un servicio o producto a la SUNASS.

5.12 Red informática: Es una red de computadoras, también llamada red de ordenadores, red de comunicaciones de datos, es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

5.13 Servicio Digital: Es aquel provisto de forma total o parcial a través de Internet u otra red equivalente, que se caracteriza por ser automático, no presencial y utilizar de manera intensiva las tecnologías digitales, para la producción y acceso a datos y contenidos que generen valor público para los ciudadanos y personas en general.

5.14 Servidor de red: Es un equipo que ofrece varios recursos compartidos de computadoras y otros servidores en una red informática.

5.15 Sistema informático: Es el sistema integrado por hardware, software y recursos humanos (administrador de la red informática, soporte técnico).

5.16 Spam: Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido (correo anónimo), habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (masivas) que perjudican de alguna o varias maneras al receptor.

5.17 Software: Equipamiento o soporte lógicos de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

5.18 Software malicioso (*malware*): Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora, ***un dispositivo móvil (laptop, celulares, tablets, etc.)*** sin el consentimiento de su propietario. Por ejemplo, virus, software espía (*spyware*), troyanos, y otras amenazas similares.

5.19 Tecnologías Digitales: Se refieren a las TIC, incluidos Internet, las tecnologías y dispositivos móviles, así como la analítica de datos utilizados para mejorar la generación, recopilación, intercambio, agregación, combinación, análisis, acceso, búsqueda y presentación de contenido digital, incluido el desarrollo de servicios y aplicaciones aplicables a la materia de gobierno digital.

5.20 Usuario/a: Es toda persona, sea funcionario o servidor público, consultor, practicante, u otro, sin importar el régimen laboral o de contratación al que esté sujeto, que ha sido debidamente autorizado para el uso de uno o varios servicios informáticos de la SUNASS.

6. DISPOSICIONES GENERALES

6.1 Es responsabilidad de todos/as los/as usuarios/as cumplir con la presente directiva y cualquier otra normativa interna relacionada a seguridad de la información.

6.2 El Oficial de Seguridad y Confianza Digital revisa la presente directiva al menos una vez al año o cuando ocurran cambios significativos, para asegurar su conveniencia; así como, propone la formulación o modificación de otros documentos de gestión interna (procedimientos, caracterizaciones, formatos, entre otros) que se requieran.

6.3 El Oficial de Seguridad y Confianza Digital difunde los lineamientos específicos de seguridad de la información para concientizar a los/as usuarios/as de la SUNASS y promover su contribución a la efectividad del SGSI.

6.4 La SUNASS, en el marco de su compromiso con la seguridad de la información, monitorea la aplicación de la presente directiva, en el marco de su SGSI.

6.5 El incumplimiento de los lineamientos específicos de seguridad de la información establecidos en la presente directiva tendrá como resultado la aplicación de las sanciones establecidas en el RISS de la SUNASS, dándose inicio al procedimiento administrativo disciplinario correspondiente y/o a las acciones legales que la ley faculte.

7. DISPOSICIONES ESPECIFICAS

7.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1.1 Los roles y responsabilidades para la seguridad de la información en la SUNASS se encuentran establecidas en la Matriz de roles, responsabilidades y autoridades del SIG (GDI-MAS-IG004), que se encuentra disponible en el portal del ***SIG*** de la SUNASS (intranet).

7.1.2 La segregación de los roles, funciones y responsabilidades de los/las usuarios/as y las áreas para la gestión de la seguridad de la información dentro de la SUNASS, se encuentran separadas con la finalidad de reducir oportunidades de modificación no autorizada o no intencional o el mal uso de los activos de la entidad.

7.1.3 La SUNASS, identifica a las autoridades pertinentes para comunicar los incidentes de seguridad de la información en la "Lista de Contactos con Autoridades y Grupos de Interés"; así como, los grupos de interés en donde tiene participación, con el fin de realizar consultas relacionadas a seguridad de la información.

7.1.4 La SUNASS integra la seguridad de la información en la gestión de proyectos, con el fin de garantizar que los riesgos de seguridad de la información sean identificados y tratados independientemente al tipo de proyecto. Además, identifica la relación de proyectos y la evaluación de sus riesgos.

7.2 DISPOSITIVOS MÓVILES

7.2.1 La asignación de los dispositivos móviles del tipo smartphone, laptops, iPad y Tablets, es registrado e inventariado por la UA.

7.2.2 Los dispositivos móviles deben contar con mecanismos de autenticación como huella digital, clave, patrón, etc.

7.2.3 Todos los/as usuarios/as que tienen asignados dispositivos móviles ***deben contar con*** la última versión o la versión más segura de los sistemas operativos que correspondan. Asimismo, ***deben contar con*** los parches y aplicaciones provenientes del fabricante.

7.2.4 Toda la información contenida en los aplicativos de la SUNASS y aquella que se haya generado por el desempeño de las funciones del personal y que se encuentre contenida en los dispositivos móviles asignadas, es de propiedad única y exclusiva de la SUNASS, y es clasificada bajo todo concepto como Confidencial.

7.2.5 ***No está permitido que el usuario formatee el dispositivo móvil asignado.***

7.2.6 Es responsabilidad de la OTI:

a) Realizar la instalación y configuración del perfil del usuario en las laptops. El/la usuario/a no cuenta con permisos para instalación o cambios de aplicaciones.

b) Establecer los requisitos de configuración y de conexión para dispositivos móviles, a fin de incluirlos cuando los dispositivos estén fuera de áreas controladas (VPN, Antivirus, parches críticos, escaneo en busca de virus, entre otros).

c) Configurar las laptops para cifrar su almacenamiento interno.

d) Configurar los dispositivos móviles para que el usuario no pueda deshabilitar o modificar la funcionalidad de seguridad, así como instalar o desinstalar aplicaciones.

e) Asegurar que todo dispositivo móvil que se conecte a la red de la SUNASS cuente con antivirus y sistema operativo actualizado.

f) Al efectuar el reemplazo de un dispositivo móvil, debe cumplir con el borrado seguro según lo establecido en el literal f) del numeral 7.5.3, el cual es ejecutado por el personal de la Mesa de Ayuda de la OTI.

7.2.7 Es responsabilidad del usuario:

a) Proteger los dispositivos móviles asignados, debe evitar dejarlo en cajones sin seguro, lugares de reunión, autos o ambientes sin supervisión; manteniéndolo en lugares que ofrezcan seguridad.

b) En el caso de Smartphone:

- ***Si cuenta con un nuevo dispositivo móvil asignado, debe requerir*** la migración de la información a la Mesa de Ayuda de la OTI.
- ***El smartphone asignado, no debe ser entregado*** a otra persona, ***especialmente cuando*** almacenan información sensible de la entidad. En estos casos, incluso los mensajes recibidos de números o remitentes desconocidos deben ser denegados y borrados sin ser abiertos.

c) Evitar conectar medios extraíbles al dispositivo móvil asignado. En caso sea necesario deben llevar el dispositivo a la Mesa de Ayuda de la OTI, para que puedan conectar el dispositivo extraíble y descargar la información para remitirlo por correo.

d) Evitar conectar los dispositivos móviles asignados a redes Wi-Fi abiertas o que no sean de confianza.

e) Bloquear su cuenta cuando deje el dispositivo móvil desatendido.

f) Almacenar la información de trabajo del dispositivo móvil (laptops, pc) asignado en la ubicación indicada por la OTI tales como: "Mis documentos", la unidad H o el OneDrive.

g) Asegurar que no se utilice el dispositivo móvil asignado de propiedad de la entidad en actividades ilegales contrarias a la moral y las buenas costumbres o para fines ajenos a las actividades propias de su función. ***El usuario es responsable de toda actividad realizada en el dispositivo móvil asignado.***

7.2.8 ***En caso de pérdida o robo, el usuario en un máximo de 24 horas debe realizar la denuncia policial respectiva y*** debe comunicar inmediatamente a él/la Jefe/a de la UA y a la Mesa de Ayuda de la OTI (mesadeayuda@sunass.gob.pe), a fin de que se realicen las acciones correspondientes.

En el caso de las laptops, la OTI debe activar el restablecimiento remoto del equipo a fin de proteger la información que contiene y limitar el acceso a los sistemas institucionales.

7.3 TELETRABAJO

Todo el personal que realiza teletrabajo parcial o total debe firmar la "Declaración Jurada sobre el Uso de Recursos, Servicios Informáticos, Confianza Digital, Protección y Confidencialidad de los Datos de la Sunass bajo la Modalidad de Teletrabajo" entregada por la URH. En este documento se establecen lineamientos que se deben cumplir con relación al uso de los sistemas de información y equipos informáticos asignados por la Sunass; así como también, para aquellos casos en el que se emplean equipos informáticos personales para el desempeño de sus funciones.

7.3.1 Es responsabilidad del personal:

a) Proteger la información, a la que tiene acceso, de amenazas como accesos no autorizados, alteración indebida o software malicioso, cumpliendo con lo siguiente:

- Debe conectarse desde ambientes físicos seguros.
- Debe bloquear el equipo informático asignado cuando se retira de su lugar de trabajo.
- Debe conectarse desde accesos a internet confiables, no públicos o gratuitos.
- Debe verificar la seguridad de las redes domésticas, es decir, que el acceso a la red inalámbrica tenga clave de acceso.
- Debe brindar acceso al personal autorizado de Mesa de Ayuda de la OTI para la actualización del sistema operativo y antivirus del equipo informático asignado, y para que las aplicaciones cuenten con las últimas actualizaciones.

- Bloquear la pantalla de su equipo de cómputo cuando no esté haciendo uso de este, o cuando por algún motivo deba ausentarse de su puesto de trabajo.
- Debe verificar que el equipo informático asignado cuente con bloqueo automático por inactividad.
- ***Debe estar ubicado en un lugar que garantice la privacidad de su trabajo, evitando que sea visible para otras personas.***
- ***En caso de pérdida o robo se debe proceder con lo indicado en el numeral 7.2.8 de esta directiva.***
- ***El usuario debe asegurarse que su equipo conectado de forma remota, no se conecte a ninguna otra red al mismo tiempo, excepto a la red personal que está bajo su control.***

b) Tomar las medidas para que el ambiente físico tenga fácil acceso a la red alámbrica o inalámbrica (WIFI), sin problemas de señal que pueda impactar en el desarrollo de su trabajo, es decir, contar con conexión a internet de alta velocidad y confiable.

c) ***Garantizar que todos los trabajos realizados en la modalidad de teletrabajo se guarden en la plataforma tecnológica de la SUNASS, por ello no se*** debe almacenar información de trabajo en los equipos informáticos asignados, solo se debe realizar en la ubicación de almacenamiento indicada por la OTI tales como: ***"Mis documentos"***, la unidad H o el OneDrive.

d) No realizar actividades ilícitas ni vulnerar los lineamientos de seguridad de la información establecidos por la SUNASS o utilizar el acceso remoto suministrado para obtener lucro comercial.

7.3.2 Es responsabilidad de la SUNASS:

a) Concientizar al personal sobre la necesidad de proteger su usuario y contraseña de acceso, y no compartirla con nadie.

b) Brindar al personal los accesos a los sistemas de información, de acuerdo con lo solicitado por los/as Directores/as y Jefes/as de cada unidad de organización de la SUNASS.

c) Asegurar que los equipos que se entreguen a los colaboradores deban contar con antivirus y Sistema Operativo actualizado.

d) Efectuar periódicamente monitoreos de las conexiones remotas, prestando especial atención a los intentos de conexión sospechosos.

e) Verificar que los equipos informáticos asignados para trabajo remoto tengan instalado y configurado correctamente el software VPN ***y la solución de administración remota autorizada por la OTI para el soporte al usuario.***

f) Verificar que la herramienta utilizada por el personal de soporte de la OTI, para el acceso remoto a los equipos del personal con modalidad de teletrabajo, sean seguros.

g) Llevar un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

h) Verificar el uso de la doble autenticación para el acceso a la infraestructura tecnológica de la SUNASS.

i) Verificar que se abandonen los accesos a los sistemas de información, cuando finalicen las actividades remotas.

7.4 SEGURIDAD DE LOS RECURSOS HUMANOS

Involucra a todos los/as usuarios/as que utilizan la información de la SUNASS para el desempeño de sus actividades.

7.4.1 **Antes del empleo:**

a) La URH es responsable del proceso de contratación de personal bajo el régimen laboral de la actividad privada (Decreto Legislativo N° 728), régimen especial de Contratación Administrativa de

Servicios (Decreto Legislativo N° 1057) y régimen especial que regula las modalidades formativas de servicios, para el cual se realiza un concurso público de méritos.

b) Para el proceso de selección, la URH aplica lo establecido en la caracterización del proceso "Selección del personal (GRH-SDP-CR-N2)".

c) En el caso de los proveedores de servicios, la UA aplica lo establecido en la Ley de Contratación del Estado y en la caracterización de los procesos "Contrataciones mayores a 8UIT relacionadas a la ley 30225 (GAF-CMR-CR-N2)" y "Contrataciones iguales e inferiores a 8UIT (GAF-CII-CR-N2)" que incluyen las etapas del proceso de evaluación y selección de proveedores, según corresponda la cuantía de la contratación.

d) Las responsabilidades del personal, de los proveedores de servicios y de la SUNASS se encuentran definidos en los contratos, términos de referencia y/o acuerdos de confidencialidad respecto a la seguridad de la información, respectivamente.

e) Para asegurar el cumplimiento de las obligaciones contractuales por parte del personal y de los proveedores de servicios, se establece:

- Cuando se requiera acceder a información sensible de la SUNASS, se deben firmar acuerdos de confidencialidad con el personal o los proveedores, según corresponda; antes de que se les otorgue acceso a las instalaciones de procesamiento de información.
- Las responsabilidades para la clasificación y gestión de la información de la SUNASS, otros activos relacionados con la información, las instalaciones de procesamiento de información y los servicios de información manejados por el personal o proveedor.
- Las responsabilidades del personal o del proveedor de servicios para el manejo de información de otras organizaciones o partes externas y las acciones a ser tomadas si el personal o proveedor incumple los requisitos de seguridad la SUNASS.

f) Todo el personal está sujeto a las cláusulas de confidencialidad, las cuales se mantienen vigentes aun cuando haya finalizado el vínculo laboral con la SUNASS.

g) El/la Jefe/a de la URH, solicita el alta de personal nuevo a la OTI, según lo establecido en la caracterización del proceso "Administración de cuentas institucionales (GTI-ACI-CR-N3)".

h) En el caso de los proveedores de servicios, los/as Directores/as o Jefes/as de las unidades de organización de la SUNASS, deben solicitar a la Mesa de Ayuda de la OTI, los accesos que, por desempeño de su servicio, deben tener a los recursos informáticos y aplicaciones.

7.4.2 Durante el empleo

a) Respecto a la conciencia, educación y capacitación sobre la seguridad de la información:

- La SUNASS promueve la toma de conciencia del personal, mediante la ejecución de reuniones, talleres de sensibilización, envío de mensajes de sensibilización y otros, de tal forma que faciliten la comprensión de temas relativos a la seguridad de la información.
- La URH, de forma anual, realiza el diagnóstico de las necesidades de capacitación (DNC) del personal de la SUNASS, con la finalidad de elaborar el Plan de Desarrollo de Personas (PDP). El PDP incluye actividades de capacitación para cerrar las brechas identificadas; el seguimiento de su cumplimiento es realizado por la URH.
- El nuevo personal de la SUNASS participa del proceso de inducción organizado por la URH, de acuerdo con lo establecido en la caracterización del proceso "Inducción (GRH-IND-CR-N2)", con la participación del Oficial de Seguridad y Confianza Digital.
- En coordinación con la OCII, se divulga mensajes de sensibilización sobre temas vinculados a la seguridad de la información, cuyo contenido es proporcionado por el Oficial de Seguridad y Confianza Digital.
- Todo el personal de la SUNASS debe asistir a las charlas, talleres o capacitaciones en Seguridad de la Información.

- Los proveedores de servicios, de ser necesario, reciben concientización en lineamientos y procedimiento relacionados a la seguridad de la información de la SUNASS.

b) Las medidas disciplinarias se rigen por la normativa aplicable y el RISS de la SUNASS. La URH ejecuta el proceso disciplinario de acuerdo con lo establecido en la caracterización del proceso "Procedimientos disciplinarios (GRH-PDI-CR-N2)".

7.4.3 **Terminación y cambio del empleo**

a) Las responsabilidades relativas a la seguridad de la información que siguen vigentes luego de la finalización de la relación contractual o el cambio del puesto de trabajo se encuentran establecidas en el contrato, términos de referencia y/o acuerdos de confidencialidad.
b) Los derechos de acceso a la información y a las instalaciones de procesamiento del personal y de proveedores de servicio, es removido o modificado al producirse el término de la relación laboral o del contrato.
c) El/la jefe/a de la URH solicita la baja del personal cesado a la OTI, según lo establecido en la caracterización del proceso "Administración de cuentas institucionales (GTI-ACI-CR-N3)".
d) En el caso de los proveedores de servicios, los/as Directores/as o Jefes/as de las unidades de organización de la SUNASS, deben solicitar a la Mesa de Ayuda de la OTI la deshabilitación de los accesos que fueron proporcionados para el desempeño de su servicio.

7.5 GESTIÓN DE ACTIVOS

7.5.1 **Responsabilidad sobre los activos**

a) Los activos de información se identifican en el "Inventario de Activos de Información" asociados a los procesos, sus propietarios y ubicación. El inventario debe ser actualizado como mínimo una vez al año o ante cualquier modificación de la información registrada, lo que suceda primero.
b) La responsabilidad de los activos de información está referida al propietario de la información y de los procesos que la manipulan, sean estos físicos o electrónicos, aunque tenga autoridad formal, no significa que tenga derechos de propiedad sobre el activo.
c) Respecto al uso aceptable de los activos:
   - El uso de los activos de información debe ser para propósitos de las actividades de la entidad, de acuerdo con los lineamientos y procedimientos que se definan y considerando criterios de buen uso.
   - No se debe divulgar información clasificada como "Confidencial" o de "Uso Interno", salvo que se cuente con la autorización expresa del Propietario del Activo de Información.
   - Cuando se requiera proporcionar información "Confidencial" o de "Uso Interno" a terceros, se debe solicitar autorización al Propietario del Activo de Información. La entrega de esta información se debe realizar suscribiendo acuerdos de confidencialidad con el tercero, y aplicando los controles específicos que se definan para tal fin.
   - Se deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo los lineamientos de seguridad que deben mantenerse alineadas con las normativas y leyes vigentes.
   - Se debe gestionar adecuadamente los elementos de control de acceso, como contraseñas (control lógico); así como, las llaves de cerradura (control físico).
   - Se aplican las sanciones establecidas en el RISS de la SUNASS al personal que ponga en riesgo los activos de información.
d) Todo el personal y los proveedores deben devolver todos los activos que la SUNASS les haya proporcionado para el desempeño de sus funciones o ejecución de su servicio al término de su contrato o servicio.

7.5.2 Clasificación de la información

a) Respecto a la clasificación:

- Los activos de información se clasifican en:
  - **Confidencial:** Es la información cuyo contenido no es divulgado ni distribuido a personas que no sean autorizadas. El acceso a esta información requiere de la aprobación del propietario y es de uso exclusivo interno de la entidad. En el caso de terceros (auditores, entidades reguladoras, consultores externos), se requiere el acuerdo de confidencialidad firmado para brindar acceso excepcional, el cual se encuentra regulado y sujeto a condiciones específicas de acceso. El acceso no autorizado a esta información podría impactar a la entidad.
  - **Uso Interno:** Es la información cuyo contenido sólo es de uso y divulgación del personal de la SUNASS. Sólo podrán ser divulgados a terceros mediante la firma de un acuerdo de confidencialidad, siempre y cuando su divulgación no impacte a la entidad.
  - **Público:** Es la información no sensible de acceso público y que su divulgación no genera impacto a la entidad.
- Los Propietarios de los Activos de Información son responsables de su clasificación, la misma que se encuentra registrada en el Inventario de Activos de Información.
- El Propietario del Activo de Información realiza la actualización del Inventario de Activos de Información en forma anual y/o cuando estime que un activo de información ha aumentado su valoración; en este caso, se cambia la clasificación del activo de información en forma inmediata, sin esperar el próximo ciclo de actualización.
- Si la información ha disminuido su sensibilidad, se podrá modificar la clasificación de forma inmediata o en el próximo ciclo de actualización. La responsabilidad de la decisión corresponde al Propietario del Activo de Información.
- Toda la información que no ha sido específicamente clasificada es considerada como “Uso Interno”, por lo que el Propietario del Activo de Información debe autorizar su acceso formalmente (a través de un correo electrónico, memorándum, entre otros).

b) Etiquetado de la información:

- Los activos de información se etiquetan según su clasificación, esto incluye información impresa y digital.
- Todos los documentos físicos o digitales que son considerados “Confidencial” o de “Uso Interno”, deben ser etiquetados (marcados), en el pie de cada página del documento, siempre y cuando los activos sean de propiedad de la SUNASS.
- Todos los envíos de información clasificada como “Confidencial” deben ser realizados por medios de transporte conocidos y seguros.
- La información con clasificación “Confidencial” que se envía por correo electrónico, debe indicar en el cuerpo del correo esta clasificación.
- Se excluye de etiquetar la salida de información de los sistemas de información de la SUNASS.

c) Respecto al manejo de activos:

- La documentación impresa y clasificada como “Confidencial”, debe almacenarse en un lugar que pueda evitar amenazas tales como accesos no autorizados, incendios o inundaciones.
- Para el caso de información clasificada como “Confidencial”, el Propietario del Activo de Información debe realizar seguimiento a los originales y copias, indicando como mínimo, el número de copias, su ubicación y a los responsables de su manejo.

- Antes de enviar dispositivos de almacenamiento a algún tercero, la información sensible debe ser removida o manejada según criterios establecidos por el propietario de la información.
- En el caso de los sistemas de información, el nivel de confidencialidad en sistemas de información, aplicaciones, formularios informáticos y bases de datos, no se encuentra indicado en la pantalla de acceso al sistema; sin embargo, los usuarios que tengan acceso y exporten la información deben seguir las reglas de etiquetado de información según el tipo de formato (documento físico, digital, correo electrónico, soporte de almacenamiento electrónico).
- ***Cada activo de información institucional (computadoras, portátiles, servidores, tablets) debe ser inventariada por la OTI.***
- ***La OTI debe verificar el inventario de los activos de información en un período no menor de 6 meses contados desde la fecha en que se realizó el ultimo inventario.***
- ***Toda adquisición de un activo de información debe tener la aprobación de la OTI.***
- ***La OTI debe mantener actualizado el listado de los proveedores de Activos de Información (Software y Hardware).***
- ***Sólo está permitido la instalación de software que haya sido aprobado por la OTI***
- ***La OTI debe revisar periódicamente el software instalado en todos los equipos de los usuarios.***

7.5.3 **Manejo de los medios removibles:**

a) Los puertos USB están restringidos para el intercambio de información.

b) Los datos institucionales no deben almacenarse en medios removibles personales.

c) Todo los medios reutilizables y su contenido que ya no son necesarios deben hacerse irrecuperables.

d) Los medios de almacenamiento se custodian en un entorno seguro según las especificaciones del fabricante.

e) En los casos que ***se disponga*** de medios removibles con información considerada como "Confidencial" o la integridad de los datos es importante, se debería utilizar técnicas de cifrado o empaquetado (ZIP o RAR) y con clave para proteger los datos en estos medios removibles/extraíbles.

f) La OTI aplica el borrado seguro de los medios de almacenamiento y se los entrega a la UA para la disposición de estos. ***El borrado seguro también se aplica en el caso que el medio removible sea reutilizado por otro personal.***

g) Se debe proteger los dispositivos usados para el resguardo de la información contra el acceso no autorizado, el mal uso o la corrupción durante el transporte, para lo cual la SUNASS debe contar con transporte o mensajeros confiables para la protección de sus activos de información.

h) Toda información confidencial en medios físicos debe contener una protección física adicional como un embalaje.

i) Los documentos confidenciales en papel considerados como desecho deben triturarse antes de retirarlos de las instalaciones de SUNASS.

7.6 CONTROL DE ACCESO

Para controlar los accesos a la información, mantener el acceso autorizado del personal y prevenir accesos no autorizados a los sistemas de información ***y/o recursos informáticos*** de la SUNASS, se establece lo siguiente:

7.6.1 ***Los requisitos descritos en este numeral se aplican a todos los sistemas, bases de datos, redes, servidores e infraestructura de la SUNASS y deben ser aplicados por todo el personal, así como por los contratistas involucrados en los accesos a la plataforma de la SUNASS.***

7.6.2 Respecto a los requerimientos para el control de acceso:

a) Todos los accesos a los activos de información lógicos deben basarse en la necesidad y rol del/de la usuario/a. Se debe tomar en cuenta los siguientes aspectos:
   - El uso de perfiles de usuarios definidos según ***necesidad y siguiendo el principio de mínimo privilegio.***
   - La revisión periódica de los controles de acceso, ***por parte del equipo de seguridad informática***.
   - La revocación de los derechos de acceso.

b) El personal de la entidad y/o terceros sólo deben tener acceso a redes y servicios a los que fueron específicamente autorizados a utilizar.

c) Todo el personal que requiera acceder ***a los servicios de*** red debe contar con las autorizaciones respectivas del responsable ***designado de la unidad en la que labora***.

d) El personal no debe almacenar información de trabajo en los equipos informáticos asignados, así como tampoco en dispositivos de almacenamiento extraíbles, solo se debe realizar en la ubicación de almacenamiento tales como: "Mis documentos", la unidad H, el OneDrive.

e) En los casos en que, por la naturaleza de su función, el personal requiera alguna excepción respecto de las disposiciones establecidas en el presente documento, esta debe contar con la autorización de su jefatura inmediata y la evaluación del riesgo asociado por parte del Oficial de Seguridad y Confianza Digital.

7.6.3 Las contraseñas seguras a los recursos de red deben de considerar lo siguiente:

a) Contar con una periodicidad de actualización de noventa (90) días.

b) No deben ser menor a ocho (8) caracteres.

c) No deben de contener datos del usuario, como nombre, apellidos, entre otros.

d) Las contraseñas no deben ser almacenadas en los exploradores de internet (Google, Chrome, Edge).

e) Deben de contener como mínimo un carácter en mayúscula, minúscula, un número ***y*** un carácter especial. Los caracteres a considerar son:
   - Mayúsculas, de la "A" a la "Z";
   - Minúsculas, de la "a" a la "z";
   - Dígitos de base 10 (del 0 al 9);
   - Caracteres no alfanuméricos, por ejemplo: ¡, $, #, %.

7.6.4 Respecto a la gestión de acceso de los usuarios:

a) La Mesa de Ayuda de la OTI, asigna cuentas de usuario de red (dominio) y correo electrónico al personal de la entidad, de acuerdo con lo establecido en la caracterización del proceso "Administración de cuentas institucionales (GTI-ACI-CR-N3)".

b) Los/as Directores/as ***y/o*** Jefes/as de las unidades de organización de la SUNASS ***o a quien designen de su unidad***, pueden solicitar a la OTI, la creación de usuarios genéricos para servicios específicos, los mismos que son reportados al Oficial de Seguridad y Confianza Digital. Es responsabilidad de los/as Directores /as y Jefes/as que solicitaron la creación del usuario genérico el comunicar a la OTI la finalización del servicio para que se realice la desactivación de la cuenta.

c) Para los sistemas o aplicaciones que como parte de su funcionalidad requieran el uso de cuentas genéricas no se requiere reportarlo al Oficial de Seguridad y Confianza Digital.

d) El/la usuario/a debe cambiar la contraseña cada noventa (90) días para poder acceder a los servicios de TI.

e) La Mesa de Ayuda de la OTI, es responsable de proporcionar a los/as usuarios/as el acceso a los recursos informáticos como impresoras, carpetas de red y demás servicios informáticos.

f) Los/as Directores/as y Jefes/as de las unidades de organización de la SUNASS, pueden solicitar a la OTI, la creación de una carpeta compartida***, en el servidor de archivos***, para el manejo de información, adjuntando la relación del personal que tendrá acceso a la misma, señalando para cada uno el nivel de acceso. Los/as usuarios/as indicados serán los/as únicos/as responsables de guardar la información institucional en dicha carpeta. Los niveles de acceso son: Lectura (consulta de información), Escritura (solo permite o deniega cambios de un archivo) y Control Total (incluye escritura, borrado y/o modificación de datos). Esta solicitud se realiza mediante la Mesa de Ayuda adjuntando el formato "Solicitud de Accesos y Privilegios a los Sistemas de Información de la SUNASS (GTI-OTI-FM001)" debidamente llenado.

g) El/la Jefe/a de la URH ***o a quien designe***, informa a la Mesa de Ayuda de la OTI, la baja de usuarios cuando el personal se desvincula de la entidad.

h) La OTI no es responsable de la gestión de usuarios de sistemas de información que no se encuentren dentro de su administración.

i) Respecto a la gestión de derechos de acceso privilegiados:

- ***Se debe administrar las cuentas con accesos privilegiados, estas cuentas tienen amplios derechos y permisos de acceso que les permiten realizar acciones críticas dentro de la infraestructura tecnológica.***
- ***Los administradores de los sistemas operativos y base de datos deben tener cuentas segregadas.***
- ***La cuenta de administrador son cuentas privilegiadas que sólo deben utilizarse para realizar actividades administrativas y no para navegación por internet, correo electrónico o actividades similares.***
- ***El especialista en seguridad informática debe identificar, inventariar y monitorear las cuentas privilegiadas con una frecuencia semestral y validar la necesidad de dichos privilegios, a fin de reasignarlos o eliminarlos de ser necesario. Dicho inventario debe incluir las cuentas de usuarios y de administrador, y como mínimo debe contener el nombre de la persona responsable, nombre del usuario, fechas de inicio y área de trabajo.***
- ***Las cuentas identificadas e inventariadas deberán ser como mínimo:***
    - ***Cuenta de administrador local.***
    - ***Cuenta de administrador de dominio y servidores Microsoft.***
    - ***Cuenta de administrador a servidores Linux.***
    - ***Cuenta de administrador de plataforma de virtualización.***
    - ***Cuenta de administrador de las bases de datos.***

  Estas cuentas deben tener habilitadas el registro de seguimiento para la auditoría correspondiente.
- ***El/la Jefe/a de la OTI designa los roles de administrador mediante la emisión de un memorando.***
- ***El inventario de contraseña de los super usuarios será almacenada por sobre lacrado y estará bajo custodia del Oficial de Seguridad y Confianza Digital.***
- ***Se deben considerar que los registros de eventos de seguridad (logs) de las cuentas privilegiadas se almacenen para que permita realizar el seguimiento a cada una de ellas.***
- ***Ningún usuario/a debe contar con privilegio de administrador, en caso sea requerido por el/la Directora/a o Jefe/a de la unidad de organización, este/a debe solicitarlo a la Mesa de Ayuda de la OTI debidamente justificado, indicando: los datos del usuario/a, fecha de***

inicio y fecha de fin del acceso (puede ser temporal y/o perenne), el cual debe contar con la autorización del/de la Jefe/a de la OTI y el Oficial de Seguridad y Confianza Digital.

- ***Los sistemas informáticos de la SUNASS no deben utilizar las cuentas privilegiadas para su operación o funcionamiento.***

j) Respecto a la gestión de la información de autenticación secreta de usuarios, la Mesa de Ayuda de la OTI, envía al usuario sus credenciales de inicio ***. Por seguridad, el usuario está obligado a cambiar su contraseña al acceder por primera vez por configuración del sistema. La Mesa de Ayuda se comunica con el usuario*** para configurar en el equipo asignado sus accesos y correo electrónico.

k) ***Cada seis meses, el Especialista en Seguridad de la Información de la OTI***, revisa los derechos de acceso de todos los usuarios para verificar si se han atendido las solicitudes de altas, bajas o modificaciones. En caso ***de identificar*** usuarios que no deben ***tener acceso*** activo o ***que requieren*** actualizar sus accesos, se ***procede a*** notificar por correo electrónico a el/la Director/a o Jefe/a de la unidad de organización que corresponda ***o a la persona responsable designada*** con copia al Oficial de Seguridad y Confianza Digital. ***Una vez recibida*** la validación del Director/a o Jefe/a de la unidad de organización ***correspondiente, se*** procede a dar de baja o actualizar ***los*** accesos ***de los usuarios***, según corresponda.

l) La baja y cambios de accesos de usuario/as se realiza de acuerdo con lo indicado en el numeral 7.4.3 de la presente directiva. ***La información, así como la cuenta del usuario debe ser almacenada por*** un periodo mínimo de tres (3) meses (tiempo de retención) ***y luego debe ser eliminada***, como consecuencia de la desvinculación de su empleo, contrato o acuerdo. ***El Especialista en Seguridad Informática de la OTI,*** mensualmente ***debe revisar*** las cuentas deshabilitadas para verificar si deben ser eliminadas de acuerdo con los tiempos de retención establecidos. ***Todas las excepciones a esta regla deberán ser comunicadas al Oficial de Seguridad y Confianza Digital.***

m) ***Se debe tener habilitado el factor de doble autenticación para todos los servicios de Microsoft y en los nuevos sistemas, de ser el caso.***

7.6.5 Responsabilidades de los usuarios:

a) Son responsables de la confidencialidad de la contraseña asignada y de las consecuencias por las acciones que terceras personas puedan hacer con el uso de esta.

b) Debe cambiar su contraseña de acuerdo ***a lo estipulado con el presente lineamiento.***

c) Las cuentas de usuarios/as se bloquean al tercer intento, para activarla deben comunicarse con la Mesa de Ayuda de la OTI.

d) No debe compartir las contraseñas asignadas, se encuentra prohibido.

e) Debe bloquear su equipo asignado, cuando se retira de su estación de trabajo.

f) ***De sospechar que la contraseña fue robada mediante phishing o algún otro tipo de ataque, debe cambiar inmediatamente la clave e informar a mesa de ayuda.***

g) ***Los usuarios no deben utilizar cuentas de propiedad personal (Hotmail, Google, etc.) en dispositivos institucionales.***

h) ***Los usuarios no deben utilizar licencias institucionales en dispositivos personales.***

i) ***Los datos institucionales no deben almacenarse en plataformas de proveedores de nube personales (Google Drive, MS Onedrive personal, Dropbox, entre otros).***

7.6.6 Respecto al control de acceso al sistema y a las aplicaciones:

a) Los accesos a la información y a las funciones del sistema deben tener controles de seguridad (por ejemplo, usuario y contraseña), a fin de evitar accesos no autorizados a recursos o información, así mismo, los derechos de acceso ya sea de lectura, escritura, borrar y ejecutar deben ser controlados.

b) Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen: el procedimiento de inicio de sesión segura, la identificación y autenticación de usuarios y la restricción del uso de herramientas utilitarias con capacidades de eludir y/o sobrescribir los controles de seguridad.
c) El uso de programas utilitarios ***que vulneren los controles de seguridad no debe ser instalados ni utilizados bajo sanción como se estipula en el RISS.***
d) Todo programa utilitario debe pasar por un proceso de identificación, autenticación y autorización de uso; así como su registro, ***en el inventario de software autorizado, por el Especialista en Arquitectura y Soluciones TI.***
e) ***Mesa de ayuda de la OTI debe desactivar y/o eliminar todo programa que no se encuentre en el inventario de software autorizado y notificar al Especialista en seguridad informática sobre estas incidencias***.
f) El acceso al código fuente de los programas sólo es accesible por los desarrolladores a su proyecto asignado, desde la plataforma de desarrollo colaborativo de software.
g) ***El área de Infraestructura debe supervisar y controlar las cuentas de acceso remoto vía VPN.***
h) ***Los visitantes que accedan a la red inalámbrica WI-FI de la SUNASS, deben acceder como usuario invitado y sólo deben tener acceso a internet limitado***.

7.7 CRIPTOGRAFÍA

Se debe emplear un listado de software NO autorizado (lista negra) para evitar su uso o un listado de software autorizado (lista blanca). El subdominio *SUNASS.gob.pe* trabaja con un certificado digital para SSL *(Secure Sockets Layer),* el cual es utilizado para el acceso a los diferentes servicios que forman parte de su plataforma. Este certificado digital, es un mecanismo que permite autenticar el sitio web en internet de manera que se conserve protegida la información de la entidad y sus clientes, puesto que, toda comunicación viajará de manera cifrada por la red.

7.8 SEGURIDAD FÍSICA Y AMBIENTAL

Estos lineamientos deben ser de conocimiento y cumplimiento de todo el personal y terceros que laboren o tengan relación con la SUNASS.

7.8.1 Respecto a las áreas seguras:

a) Para determinar un área segura se deben tener en consideración los siguientes criterios: Dónde se procesa información, dónde se almacena información y dónde se cuenta con información confidencial; asimismo se cuenta con relación de las áreas seguras.
b) En el caso que amerite, el perímetro de seguridad física estará claramente definido. Las especificaciones técnicas de seguridad dependerán del nivel de protección que se requiera implementar.
c) Las áreas donde funcionan las instalaciones de procesamiento de información y cualquier otra que sea considerada como crítica y que pudiera afectar el funcionamiento de los sistemas de información son protegidas de accesos no autorizados.
d) Las instalaciones de procesamiento de información son físicamente sólidos; los muros, paredes y pisos externos son sólidos y todas las puertas exteriores están protegidas contra accesos no autorizados mediante mecanismos de control.
e) La entidad cuenta con controles que aseguran el acceso físico sólo al personal debidamente autorizado. Se cuenta con personal de vigilancia, que verifica la autorización de ingreso a las instalaciones y registra el acceso.
f) Respecto a las oficinas, áreas e instalaciones:
- Existen controles de seguridad física.

- El personal autorizado (personal, proveedores y terceros) no debe facilitar el acceso a las instalaciones a personas desconocidas.
- Las áreas dedicadas al procesamiento de información deben ser ubicadas en un lugar que no presente riesgos desde el punto de vista de acceso al público.
- El control de acceso a los cuartos de comunicaciones de la entidad se realiza previa autorización.
- El ingreso al *Datacenter* debe ser autorizado, los visitantes deben registrarse en el formato de registro de visita.
- ***Para*** el ingreso al Datacenter debe existir el control de acceso biométrico.
- Se cuenta con video vigilancia (cámaras de seguridad) en las instalaciones.

g) Los equipos se encuentran ubicados y protegidos de tal forma que se reducen los riesgos como resultado de las amenazas externas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.
Los equipos de red y los equipos de comunicaciones (*Switches*, *Routers*, *Access Point*) ubicados dentro del *Datacenter* y en los cuartos de comunicaciones están conectados a una unidad de alimentación eléctrica por batería UPS (Sistema de Alimentación Ininterrumpida) con autonomía mínimo de una hora y un respaldo de un grupo electrógeno automático (TTA).

h) Las actividades realizadas en las áreas identificadas como seguras deben ser supervisadas para evitar amenazas.

7.8.2 Equipos

a) Respecto al emplazamiento y protección de los equipos:
- Los equipos se encuentran ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.
- La computadora personal es de uso exclusivo para los/as usuarios/as de la SUNASS para el desarrollo de sus actividades y fines de la entidad, siendo responsable de su buen uso.
- El personal debe respetar y no modificar por ningún motivo la configuración de hardware y software establecida por la OTI.
- El personal está prohibido de abrir los equipos de cómputo o dispositivos informáticos, excepto el personal especializado de la OTI.
- Las computadoras personales de la entidad no deben ser alterados (cambios de procesador, adición de memoria o tarjetas) sin evaluación técnica y autorización de la OTI.

b) Respecto a la seguridad del cableado:
- El cableado de energía o de telecomunicaciones se encuentra protegido de cualquier intercepción o daño.
- El cableado de suministro de energía eléctrica en las zonas de tratamiento de información cuenta con un sistema de puesta a tierra (pozo a tierra), el que es revisado anualmente para garantizar su adecuado funcionamiento.
- El equipo de tecnológica de la OTI debe velar que el cableado estructurado cumpla con las normas internacionales aprobadas por la TIA-EIA (Asociación de Industrias de Telecomunicaciones y Asociación de Industrias Electrónicas).

c) El mantenimiento de los equipos se ejecuta de acuerdo con lo establecido en la caracterización de proceso "Mantenimiento y Soporte de la Infraestructura Tecnológica (GTI-MSI-CR-N2)".

d) Los equipos informáticos (PC's, laptops, discos externos, etc.) de propiedad de la SUNASS, deben contar con la autorización expresa de la UA para su retiro.

e) El uso de equipos de propiedad de la SUNASS fuera de sus instalaciones debe ser autorizado de manera expresa por los/as Directores/as y/o Jefes/as de cada unidad de organización. El personal autorizado asume la responsabilidad de la custodia del equipo.
f) Se deben verificar todos los equipos para asegurar que cualquier dato sensible y software con licencia se haya eliminado antes de su reutilización o cuando se disponga su eliminación.

7.9 ESCRITORIO Y PANTALLAS LIMPIAS

Para la protección de cualquier tipo de información, en cualquiera de sus formas y que pueden estar contenidas en escritorios, estaciones de trabajo, computadores portátiles, medios ópticos, medios magnéticos, documentos físicos y en general cualquier tipo de información que es utilizada por el personal y terceros, se establece que:

7.9.1 Los lugares de trabajo de los/as usuarios/as deben localizarse preferentemente en ubicaciones que no queden expuestas al acceso de personas externas. De esta forma, se protege tanto el equipamiento tecnológico como los documentos que pudiera estar utilizando el/la usuario/a.

7.9.2 Los equipos que queden ubicados cerca de zonas de atención o tránsito de público deben situarse de forma que las pantallas no puedan ser visualizados por personas externas.

7.9.3 Toda vez que un/a usuario/a se ausenta de su lugar de trabajo debe de bloquear su estación de trabajo, así estas tengan instaladas protectores de pantalla. En el caso que no lo realice el usuario, el equipo debe de bloquearse a los 15 minutos.

7.9.4 Respecto a escritorios limpios:
a) Toda vez que un/a usuario/a se ausente de su lugar de trabajo debe guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información.
b) Al finalizar la jornada de trabajo, el/la usuario/a debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.
c) Cuando se imprima información confidencial, debe retirarse de forma inmediata de las impresoras.

7.9.5 Respecto a las pantallas limpias:
a) Las estaciones de trabajo y equipos portátiles tienen bloqueo automático en un lapso de 15 minutos.
b) La pantalla de autenticación a la red debe requerir solamente la identificación de la cuenta y una contraseña.
c) Toda vez que el/la usuario/a se ausente de su lugar de trabajo debe bloquear su estación de trabajo o laptop de forma de proteger el acceso a las aplicaciones y servicios de la SUNASS.
d) En la pantalla de los equipos no se debe tener íconos o accesos directos a carpetas o documentos de la SUNASS para proteger su integridad y confidencialidad.

7.10 SEGURIDAD DE LAS OPERACIONES

7.10.1 Para garantizar la operación correcta y segura en las instalaciones de procesamiento de información de la entidad, minimizar el riesgo de fallos de los sistemas, proteger la integridad de software y de la información, así como, monitorear las actividades de procesamiento de información para detectar acciones no autorizadas, se prohíbe expresamente:
a) Introducir en los sistemas de información o la red contenidos obscenos, amenazadores, inmorales y ofensivos.
b) Introducir voluntariamente en la red cualquier tipo de *malware*, dispositivos lógicos, dispositivos físicos, o cualquier tipo de secuencia de órdenes que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los recursos informáticos.

c) Intentar distorsionar o falsear los registros "logs" de los sistemas de información.
d) Poseer, desarrollar o ejecutar programas que pudieran dañar o alterar los recursos informáticos de la entidad.

7.10.2 La SUNASS controla la documentación de sus procesos en el "Listado Maestro de Documentos", que se encuentra disponible en su portal del SIG (intranet).

7.10.3 Todo cambio en los procesos, sistemas o instalaciones de procesamiento de la información que afecte a la seguridad de la información debe ser registrado. Para los cambios relacionados a tecnología se debe considerar lo siguiente:

a) El jefe de la OTI debe definir todas las funciones y responsabilidades junto con los coordinadores de la OTI, para garantizar un control satisfactorio de todos los cambios, que debe incluir, entre otros:

- ***Los criterios de aceptación se establecen en coordinación con el propietario del activo.***
- ***La evaluación de riesgos de la propuesta de los nuevos cambios importantes es realizada por el Especialista en Seguridad Informática.***
- ***Los cambios de emergencia en instalaciones, sistemas o aplicaciones sólo se utilizan en circunstancias extremas con la aprobación del/de la Jefe/a de la OTI.***
- ***Los parches para resolver errores de software sólo se aplican cuando se verifica que sea necesario y con la autorización del equipo técnico, la administración y el proveedor de ser el caso.***

b) En el caso de instalación de actualizaciones de software para servidores y estaciones de trabajo:
- Todas las actualizaciones deberán realizarse fuera del horario laboral.
- Las actualizaciones del sistema operativo del servidor se descargan en forma manual y mediante configuración, las actualizaciones se realizan fuera del horario laboral, de igual forma, las actualizaciones de la base de datos.
- Como buena práctica se debe considerar las recomendaciones del fabricante del S.O. con respecto a la aplicación de las actualizaciones.

c) En el caso de cambios en las configuraciones de los equipos de comunicación:
- Los cambios en las configuraciones que tengan impacto en los equipos de comunicación *router* o switches, se deben programar fuera del horario laboral, a fin de no afectar los servicios de la red.
- En caso de una actualización del *firmware*, se debe evaluar las mejoras en la seguridad o performance del equipo antes de proceder a su aplicación, considerándose en todos los casos el realizar una copia de seguridad de todas las configuraciones aplicadas al equipo como paso previo.

d) En el caso de cambios en configuraciones de equipos de seguridad:
- El equipo de infraestructura tecnológica de la OTI es responsable de la administración y monitoreo de las soluciones de seguridad basadas en hardware y/o software respectivamente; este equipo debe revisar de manera semestral las actualizaciones de seguridad que los fabricantes publican a fin de evaluar y programar su instalación.
- El/la Jefe/a de la OTI, debe coordinar con el encargado de infraestructura tecnológica la fecha y hora para que todo cambio se realice sin que afecte a los servicios de la entidad. Una vez realizado el cambio, debe enviar un correo electrónico a él/la Jefe/a de la OTI con copia al Oficial de Seguridad y Confianza Digital, indicando que se ejecutó el cambio correctamente o que no se pudo ejecutar lo solicitado, este último en caso de error en la ejecución.

- El/la encargado/a del servicio procede a realizar las pruebas y verificaciones para validar el correcto funcionamiento, de existir algún problema, se solicita el *rollback* y se reprograma la actualización.

7.10.4 Respecto a la gestión de la capacidad, se supervisa el uso de los recursos de los servidores y se hacen proyecciones de los futuros requisitos de capacidad tecnológica para asegurar el desempeño requerido de los sistemas de información, para lo cual se debe realizar lo siguiente:

a) Se identifican los requerimientos de capacidad teniendo en cuenta la criticidad del sistema para la entidad.
b) Se realizan proyecciones de los nuevos requisitos ***de capacidad para todas las actividades nuevas*** para el aprovisionamiento de recursos.
c) El Propietario del Activo debe de realizar depuraciones periódicas de datos obsoletos en disco.
d) La OTI debe desinstalar aplicaciones, sistemas, bases de datos o entornos en desuso, ***como resultado de la revisión periódica con la aprobación del Propietario del Activo.***
e) Se debe restringir el uso del ancho de banda para servicios no críticos que consumen más recursos, como es el caso de los videos, limitando el acceso a redes sociales y youtube, toda excepción debe ser autorizado por el/la Jefe/a de OTI en coordinación con el Oficial de Seguridad y Confianza Digital
f) El/la coordinador/a de infraestructura debe reportar de manera periódica los resultados de la gestión de la capacidad de la infraestructura tecnológica.

7.10.5 Respecto a la separación de los entornos de desarrollo, pruebas y producción:
a) Los ambientes de desarrollo, prueba y producción se encuentran en las oficinas de la entidad, estos cuentan con el nivel de separación necesario para prevenir problemas operacionales, así como los controles de acceso adecuados para cada uno de ellos.
b) El acceso a los ambientes de desarrollo es restringido y exclusivamente para el personal encargado de desarrollo en la SUNASS.
c) El acceso al ambiente de pruebas es restringido y exclusivamente para el personal encargado del aseguramiento y control de la calidad.
d) El personal de la OTI es responsable de la administración, mantenimiento, operatividad continua, seguridad y rendimiento aceptable de los ambientes de desarrollo, pruebas y producción.
e) Las pruebas se realizan utilizando datos de prueba, en los casos en los que, no se pueda recrear los datos de prueba y la entidad así lo requiera, la copia de datos de producción puede ser usada para las pruebas, siempre y cuando, el uso esté autorizado y analizado por el Propietario del Activo de Información y previamente tratada para el resguardo de los datos.
f) Los cambios en los sistemas de información deben ser ejecutados o automatizados por el área de Infraestructura en el entorno de producción y deben de contar con la aprobación del/ de la Jefe/a de la OTI.

7.10.6 Respecto a la protección contra códigos maliciosos:
a) Para reducir la presencia de software maliciosos en los sistemas de información y los medios de procesamiento, el sistema de ***protección de códigos maliciosos*** debe encontrarse habilitado en los equipos de la entidad; así como, en los equipos de personal de terceros o visitas que requieran ingresar a la red de la entidad.
b) El sistema de ***protección de código malicioso*** debe contar con una actualización periódica y configurada para realizar revisiones programadas para la detección de virus en los equipos de la entidad.

c) La OTI es responsable de instalar, configurar, monitorear y controlar el sistema de ***protección de código malicioso*** en las estaciones de trabajo.
d) Todo incidente de infección de virus informático debe ser reportado inmediatamente a la Mesa de Ayuda de la OTI (mesadeayuda@sunass.gob.pe) para su revisión, el cual evitará que se propague a la red informática y éste, a su vez, lo comunica al Oficial de Seguridad y Confianza Digital.
e) El usuario no debe abrir archivos adjuntos a un correo electrónico que provengan de una fuente desconocida, sospechosa o no confiable.
f) Todos los usuarios deben reportar a Mesa de Ayuda de la OTI los correos spam, cadenas u otros correos electrónicos no deseados y luego eliminarlos.

7.10.7 Sobre el respaldo de la Información:
a) Los/as usuarios/as son responsables de poner su información institucional en la unidad compartida de red y de guardar la información en el repositorio establecido por la OTI para su respaldo automático.
b) El respaldo y las pruebas de recuperación de la información se realizan según lo establecido en la caracterización del proceso "Respaldo y restauración de la información (GTI-RRI-CR-N2)" y en el instructivo de "Ejecución del respaldo y restauración de la información (GTI-OTI-IN002)".
c) Para las pruebas de restauración aleatorias se priorizan los sistemas y activos de información que son críticos para la SUNASS de acuerdo con el alcance del SGSI.

7.10.8 Respecto a los registros, monitoreo y conservación:
a) Se monitorean los servidores administrados por la OTI. Los tipos de eventos de advertencias y errores generados por el servidor son registrados y monitoreados. Cuando los eventos, tengan impactos a los servicios brindados, se deben registrar como incidentes de seguridad.
b) Los registros de eventos (log) se consolidan y protegen contra alteración, eliminación y/o accesos; para ello, se cuenta con controles de acceso a los repositorios. Los logs, tal como los otros recursos, cuentan con controles de acceso, de acuerdo con ello, solo pueden acceder los usuarios privilegiados. Estos logs no pueden ser modificados por usuarios no privilegiados.
c) Todas las actividades de los/as usuarios/as con rol de administrador, son registradas y esos registros son protegidos. Asimismo, el super administrador del servicio revisa regularmente las actividades de los administradores.
d) Todos los equipos de la red se conectan al servidor de dominio para su sincronización de actualización de los relojes y se verifica con la hora de *Google*.

7.10.9 Restricciones sobre la Instalación de software:
a) Los softwares institucionales no deben utilizarse para actividades personales.
b) Bajo ninguna circunstancia los usuarios deben descargar, instalar, copiar, acceder, ejecutar o emplear cualquiera de los siguientes:
- ***Software o programas ilegales.***
- ***Aplicaciones sin licencia.***
- ***Sistemas operativos no probados o sin licencia.***
- ***Software pirateado.***
- ***Software adquirido para uso personal o doméstico.***

c) Se debe revisar el software instalado y las licencias que se han adquirido para asegurar que solo el Software aprobado se está utilizando, como mínimo una vez al año; así como, mantener un registro de la lista de software permitidos, la cual se debe mantener actualizada.
d) En ningún caso los usuarios podrán realizar copias de los softwares institucionales para uso personal.

e) Se debe desinstalar todo el software sin licencia o cualquier software que no aparezca en la lista de software aprobado y compatible. Así mismo desinstalar el software que ya no se usa en los equipos.

7.10.10 Gestión de Vulnerabilidades técnicas

a) El análisis de vulnerabilidades técnicas de los sistemas de información en uso y de la infraestructura tecnológica, se debe realizar una vez al año con un proveedor externo, de ser posible.
b) Los hallazgos y recomendaciones de esta revisión deben ser analizadas e implementadas, de ser el caso.
c) El encargado de infraestructura tecnológica de la OTI debe ejecutar el análisis o escaneo de la red informática, la auditoría de seguridad de la red, actualizaciones de los sistemas operativos y análisis de vulnerabilidad; así como, de reportar a él/la Jefe/a de la OTI sobre el estado de la red informática de la entidad.
d) Para el caso de desarrollo de las aplicaciones, el encargado de desarrollo de la OTI debe aplicar el aseguramiento y control de la calidad, previo pase a producción, con el análisis de vulnerabilidades de acuerdo con los lineamientos establecidos por la OTI.
e) Los/a usuarios/as no cuentan con acceso para instalar aplicativos en sus equipos, el personal de la Mesa de Ayuda de la OTI debe realizar la instalación de los aplicativos, previa autorización de el/la Director/a o Jefe/a de la unidad de organización que corresponda.
f) ***Se deben realizar pruebas de seguridad y escaneo de vulnerabilidades técnicas de las aplicaciones***.

7.10.11 Controles de auditoría de sistemas de información:

a) Se debe planificar y acordar los requisitos y actividades de auditoría de sistemas de información que implican la verificación de los sistemas operativos, para minimizar las interrupciones en los procesos de la entidad.
b) Se debe controlar el alcance de las verificaciones, estas deben limitarse a accesos de sólo lectura al software y a los datos; en caso de que las verificaciones afecten la disponibilidad del sistema, deben realizarse fuera de horario laboral.
c) Todo acceso a los sistemas debe ser supervisado y registrado para poder realizar revisiones posteriores.
d) El personal de mesa de ayuda debe identificar los tipos de eventos y debilidades tomando como base el instructivo "Atención de eventos y debilidades de seguridad de la información (GTI-OTI-IN001)", para el registro y derivación al Oficial de Seguridad y Confianza Digital.
e) Los registros de los servicios críticos (logs del sistema) deben se consolidados y almacenados en una plataforma, estos deben ser conservados por un periodo de 6 meses.

7.11 SEGURIDAD DE LAS COMUNICACIONES

Para implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos con terceros, proteger la información de las redes y la protección de la infraestructura que la soporta, se establece:

7.11.1 Respecto a la gestión de seguridad de la red:

a) Todos los servidores de red que están conectados a la red informática son de acceso restringido y exclusivamente para el personal técnico especializado de la OTI.
b) Los incidentes de seguridad detectados en los ambientes gestionados son notificados a la mesa de ayuda para la toma de las acciones respectivas.
c) El encargado de infraestructura tecnológica de la OTI debe administrar, monitorear, controlar las redes de cómputo, garantizar la seguridad de la información en la red y proteger los servicios

conectados a la red; así como, es responsable de la configuración de la red cableada e inalámbrica y garantizar la disponibilidad de los servicios a su cargo.

d) En los equipos de los usuarios nuevos deberá mostrarse un banner al encender el equipo, el mensaje debe ser: Está usted accediendo a la plataforma tecnológica de la SUNASS, Señores Usuarios se les recuerda que para solicitar, servicios de Sistemas e Informática o reportar incidencias, debe generar su ticket: mandando un correo a mesadeayuda@sunass.gob.pe o ingresando a https://mesadeayuda.sunass.gob.pe:8080/

e) El encargado de infraestructura tecnológica de la OTI debe revisar los eventos detectados en el Firewall, tales como IP´s sospechosas, registrarlos en la lista negra de IP y comunicarlos al Oficial de Seguridad y Confianza Digital.

f) La seguridad en los servicios de las redes es administrada y gestionada por personal de infraestructura tecnológica de la OTI.

g) Los equipos de comunicaciones cumplen los requisitos mínimos de seguridad establecidos.

h) En la red interna se tiene habilitado la red de WIFI y solo tienen acceso los usuarios de red.

i) La red interna se encuentra segregada, para ello se configura redes virtuales (VLAN) en el *switch*, que permite la comunicación entre los/as usuarios/as y acceso a Internet.

j) El acceso inalámbrico está protegido mediante contraseñas complejas.

k) El acceso inalámbrico para las visitas sólo tiene acceso a internet y no a la red de la institución, la contraseña de esta red debe ser cambiada trimestralmente.

7.11.2 Respecto a la transferencia de información:

a) La SUNASS ha establecido controles internos para asegurar que la información transmitida dentro de la entidad esté protegida, para lo cual se cuenta con lineamientos de responsabilidades de los usuarios, controles de accesos, lineamientos de uso aceptable de activos de información. Además, se cuenta con ***sistema de protección de código malicioso*** para prevenir ***virus, malwares, entre otros.***

b) En el caso que se realice un intercambio de información con cualquier entidad externa, se debe mantener la seguridad en el intercambio de información. Asimismo, cualquier entidad externa que quiera conectarse a un *web service*, debe utilizar la conexión de Internet y tener un acuerdo de confidencialidad firmado.

c) ***Para la transferencia de información interna sólo debe realizarse mediante la plataforma de SUNASS (OneDrive) no se debe hacer uso de almacenamiento externo como Dropbox, WeTransfer, entre otros.***

d) Para la transferencia de información, se deben realizar acuerdos de transferencia segura de información entre la SUNASS y las entidades externas. Ambas deben contar con accesos y credenciales del cual compartirán información y se rigen bajo los acuerdos de confidencialidad y no divulgación de la información establecida.

e) El servicio de correo electrónico que se brinda al personal es de propiedad exclusiva de la SUNASS, tanto el correo electrónico, como su contraseña son confidenciales, personales e intransferibles. La SUNASS se reserva el derecho de activar las opciones de auditoría sobre los mensajes enviados o recibidos para verificar el cumplimiento de los lineamientos establecidos para el uso del correo electrónico.

f) ***El correo electrónico está sujeto a las mismas restricciones de uso y al mismo proceso de revisión que cualquier otro recurso proporcionado por SUNASS para el uso de los colaboradores.***

g) El personal de la SUNASS debe asegurar que ninguna persona ajena utilice su correo electrónico violando las políticas de seguridad, que no se realice actividades ilegales y que no utilice el acceso para fines ajenos a la entidad. El personal es responsable de todas las actividades realizadas con su cuenta de correo electrónico.

h) ***No está permitido la distribución intencional de spam, phishing, cadenas, anuncios, mensajes obscenos o amenazantes mediante el correo electrónico.***
i) ***Los usuarios no deben enviar, reenviar y/o responder a grandes listas de distribución relacionadas con temas no institucionales.***
j) El Oficial de Seguridad y Confianza Digital, como parte de la gestión de incidentes de seguridad, debe realizar investigaciones y tomar las acciones necesarias, en coordinación con los responsables de las unidades de organización de la SUNASS que corresponda.
k) Todo el personal y proveedores (que aplique) cuentan con acuerdos de confidencialidad o no-divulgación" los cuales detallan los aspectos de seguridad que deben de cumplir. Las obligaciones de confidencialidad inician una vez firmado este acuerdo, permaneciendo después del cese de labores, término de contrato o servicio, y extendiéndose de manera permanente.
l) Los acuerdos de confidencialidad y/o no divulgación se revisan anualmente o cuando lo requiera la SUNASS, para verificar que los requisitos de seguridad son los adecuados o pertinentes de acuerdo con sus necesidades.

7.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

Para garantizar que la seguridad de la información sea parte integral de los sistemas de información en todo el ciclo de vida, incluyendo los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas, se establece que:

7.12.1 Requisitos de Seguridad de los Sistemas de Información:

a) La SUNASS para todos los sistemas desarrollados, determina (si aplica) los requerimientos de seguridad de información antes de comenzar la fase de desarrollo, con el fin de evitar o minimizar fallas de seguridad en los sistemas de información. El coordinador de desarrollo tecnológico de la OTI debe validar si se cumplen con los requerimientos de seguridad establecidos; estos se deben establecer desde el requerimiento del/de la usuario/a. Estos requerimientos deben ser incorporados en cada fase del ciclo de desarrollo como son: Análisis de requerimientos, Diseño, Desarrollo, Pruebas e Implantación.
b) Para los sistemas web desarrollados y utilizados en la SUNASS un requisito mínimo de seguridad es que los/as usuarios/as deben estar sincronizados con el Active Directory administrado por la OTI.
c) La información involucrada en los servicios de aplicación que pasan a través de redes públicas es protegida de acuerdo con los requerimientos de seguridad definidos en el punto anterior, como también con la aplicación de protocolos como https.
d) La información implicada en las transacciones de los servicios de aplicación se protege para prevenir la transmisión incompleta, la omisión de envío, la alteración del mensaje, la divulgación, la duplicación o repetición del mensaje no autorizados.

7.12.2 Respecto a la seguridad en los procesos de desarrollo y soporte:

a) En el numeral 7.13 de la presente directiva se describen los lineamientos de desarrollo seguro, el cual está basado en los siguientes principios:
   - Partir de un mínimo modelo de permisos y luego ir escalando privilegios;
   - Limpiar la codificación de pruebas.
   - Aplicar validaciones para el registro de datos según corresponda.
   - Hacer seguimiento de las versiones y tecnologías usadas ya que estás van evolucionando o se vuelven obsoletas.
   - Las claves pasan por un proceso de encriptación.

- Los cambios que se soliciten deben pasar por un proceso de evaluación y deben ser documentados.

b) Se cuenta con la plataforma de desarrollo colaborativo de software que permite gestionar y controlar los cambios realizados que finalmente modifican el ambiente productivo siendo un requerimiento fundamental para realizar dichas modificaciones. Se deben realizar las revisiones de la funcionalidad con respecto a seguridad de la información en la fase de pruebas.

c) Para la revisión técnica de aplicaciones después de cambios en la plataforma operativa:
- Se debe verificar y garantizar que los cambios realizados en los sistemas operativos no tengan un impacto adverso en las actividades y operaciones críticas de la entidad.
- Se deben realizar pruebas funcionales de los sistemas con la finalidad de evidenciar posibles inconvenientes o incumplimiento de los requisitos de seguridad de la información establecidos.
- En caso las funcionalidades no satisfagan los requerimientos mínimos de seguridad, el encargado de desarrollo de la OTI debe comunicar las deficiencias de seguridad encontradas al encargado de infraestructura tecnológica de la OTI, para su atención.

d) Las modificaciones a paquetes de software deben limitarse solo a cambios necesarios y todos los cambios deberían ser estrictamente controlados y almacenados en la plataforma de desarrollo colaborativo de software. La OTI, como responsable del mantenimiento del software, debe considerar el impacto ocasionado a consecuencia de los cambios.

e) Los principios de ingeniería de sistemas seguros se encuentran establecidos en el numeral 7.13 de la presente directiva, el cual está basado en:
- Las aplicaciones cuentan con mecanismos de autenticación difíciles de vulnerar.
- En los casos que se requiera, aplicar el uso correcto de la criptografía.

f) Sólo las personas autorizadas del equipo de desarrollo de la OTI tienen acceso al ambiente de desarrollo seguro.

g) La OTI supervisa y realiza el seguimiento de las actividades de desarrollo de sistemas ***contratados como terceros***, establecidos en los términos de referencia:
- El acuerdo de licencias, la propiedad del código y los derechos de propiedad intelectual relacionado con el contenido de terceros.
- Los requisitos contractuales para el diseño, la codificación y las pruebas seguras.
- Las pruebas de aceptación para la calidad y precisión de los entregables.
- La presentación de pruebas de que se probaron los requisitos de seguridad para establecer los niveles mínimos aceptables de seguridad y calidad.

h) Para validar el cumplimiento de los requerimientos del usuario se realizan pruebas del sistema, de acuerdo con lo establecido por la OTI para el desarrollo de softwares. El responsable de las pruebas debe revisar el cumplimiento de los requerimientos de seguridad establecidos en la solicitud de cambios o nuevos requerimientos de sistemas.

7.12.3 Respecto a los datos de prueba:

a) Cuando se requiera migrar datos del ambiente de producción hacia el ambiente de desarrollo, de ser necesario, deben usar mecanismos de protección de datos, con la finalidad de utilizarlos en las diversas etapas de los proyectos.

b) Esta actividad se realiza a demanda y para ello, el responsable del proyecto, de ser necesario, debe solicitar autorización al usuario líder, mediante una solicitud que debe contener como mínimo: el nombre y cargo del solicitante, fecha, nombre del sistema, descripción de información requerida y el motivo de la extracción de la información especificada.

7.12.4 ***Adquisición de Sistemas de información:***

a) Se debe considerar los requisitos de seguridad de la información en la adquisición de nuevos sistemas de información o mejoras de los existentes.

b) Debe considerar los siguientes controles de seguridad:

- ***Validación y verificación de credenciales de usuario.***
- ***Firmas digitales y cifrado de la información.***
- ***Protocolos de comunicación seguros.***

c) Cualquier desarrollo contratado debe se estrictamente controlado y monitorizado.

d) Se debe aplicar controles de seguridad basados en una "Evaluación de riesgos".

e) Se deben revisar el cumplimiento de obligaciones/expectativas legales.

7.13 DESARROLLO SEGURO

La SUNASS ejecuta los proyectos de desarrollo y mantenimiento de aplicaciones en base al ciclo de vida del software se considera lo siguiente:

a) Se debe asegurar el entorno de desarrollo considerando que los miembros del equipo de desarrollo son los únicos que tienen acceso autorizado al mismo.

b) Se debe determinar el ciclo de vida de desarrollo de software, ***aplicable al proyecto de desarrollo.***

c) Los entornos de desarrollo, pruebas y producción deberán estar segregados.

d) Se deben recolectar las necesidades del usuario para desarrollar sus requerimientos y priorizarlos, se establece los requerimientos del producto y se identifican las interfaces tempranamente.

e) Las aplicaciones deben ser desarrolladas utilizando lenguajes y técnicas de programación segura, tomando en cuenta los lineamientos específicos de control de accesos.

f) En el desarrollo de aplicaciones WEB, se debe utilizar el estándar de verificación de seguridad de aplicaciones OWASP (top 10).

g) Las aplicaciones web deben utilizar consultas parametrizadas o procedimientos almacenados u ORM, en lugar de consultas embebidas en el código, para las interacciones con bases de datos.

h) El desarrollo y modificación de software sólo se debe llevar a cabo en entornos de desarrollo seguros y dichos cambios deben ser custodiados y versionados.

i) Los datos de los entornos de producción no deben utilizarse en el entorno de desarrollo o prueba, a menos que el entorno esté protegido al mismo nivel que el entorno de producción y cuente con la autorización del dueño del activo para su autorización.

j) Se debe evitar el acceso no autorizado a las fuentes del software, debiendo el acceso a dichos repositorios ser controlado.

k) Los programas fuentes se almacenan en repositorios seguros en la plataforma de desarrollo colaborativo de software, para el control de las versiones de los sistemas.

l) Todas las aplicaciones web se deben ofrecer exclusivamente mediante HTTPS.

m) Los registros de eventos de aplicaciones web se almacenan de forma centralizada.

n) Para el desarrollo de aplicaciones se utilizan las prácticas de DevOps.

o) Se ***debe validar*** el producto con la finalidad de demostrar su correcto funcionamiento en el ambiente de producción para el cual ha sido planeado. Esta validación involucra la selección de productos, el establecimiento del ambiente de validación y realizar la validación siguiendo procedimientos y criterios establecidos, los resultados deben ser analizados. La validación del producto debe ser realizada por el/la usuario/a o sus representantes formalmente autorizados.

p) Para los sistemas utilizados en la SUNASS se debe cumplir con los siguientes requisitos mínimos de seguridad:

- ***Verificar que los controles de acceso fallen de forma segura, es decir, no se emitan mensajes de error o rastros de pilas que contengan datos sensibles que podrían ayudar a un atacante,***

incluyendo el identificador de sesión, versiones de software/entorno y datos personales. Las fallas deben ser identificadas por ID y documentadas en los manuales de la aplicación.

- ***El sistema debe permitir la gestión de usuarios, grupos de usuarios y asignación de roles y perfiles, permitiendo asociar las acciones disponibles en el sistema a los roles de usuario y parametrizar las funcionalidades que cada actor puede usar en el sistema. Los permisos de acceso al sistema para los usuarios podrán ser cambiados solamente por el administrador de acceso a datos.***
- ***Un usuario puede estar asociado a uno o más roles, de tal manera que los menús de navegación del sistema se muestran o despliegan dependiendo de las acciones asociadas a cada rol de usuario, permitiendo así que cuando el usuario es autenticado correctamente el sistema verifica los roles que tiene activos para otorgarle únicamente las acciones autorizadas a realizar.***
- ***El sistema debe integrarse con LDAP (Lightweight Directory Access Protocol) para los procesos de inicio de sesión y autenticación. El sistema debe soportar la integración Nativa con Active Directory de Microsoft. Para usuarios externos (por ejemplo: vigilados y ciudadanos) el mecanismo de autorización, autenticación y acceso será controlado a través del modelo de seguridad del sistema de información.***
  El sistema debe incluir controles de bloqueo de cuenta después de un máximo de 3 intentos erróneos a fin de evitar ataques de fuerza bruta.
- ***Verificar que el identificador de sesión nunca se revele en URLs, mensajes de error o registros de bitácora. Esto incluye verificar que la aplicación sea compatible con la re-escritura de URL incluyendo el identificador de sesión.***
- ***Verificar que toda autenticación exitosa y re-autenticaciones generen un nuevo identificador de sesión.***
- ***Verificar que los identificadores de sesión son suficientemente largos, aleatorios y únicos para las sesiones activas.***
- ***Verificar que todas las consultas de bases de datos, procedimientos almacenados y llamadas de procedimientos almacenados están protegidas por la utilización de declaraciones preparadas o parametrización de consultas, y por lo tanto no sean susceptibles a la inyección de SQL.***
- ***Verificar que datos almacenados del cliente no contengan información sensible o información personal identificable.***
- ***El sistema debe permitir la implementación de certificados digitales, es decir, encriptar las comunicaciones de los servicios expuestos en internet o cualquier red otra red pública, haciendo uso de protocolos como HTTPS, SSL, entre otros. El sistema debe utilizar: certificados internos, cuando los sistemas de información vayan a ser consultados únicamente al interior de la entidad y certificados válidos públicamente, cuando los sistemas de información estén expuestos a internet.***

7.14 SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES

Para garantizar la protección de los activos de información de la SUNASS que son accesibles por los proveedores, se establece que:

7.14.1 A todo proveedor que presta servicios a la entidad, que tenga acceso a los activos de información y/o instalaciones de procesamiento, se le debe enviar las disposiciones de seguridad de la información para proveedores. El proveedor debe presentar al inicio de sus actividades el formato de Declaración jurada de compromiso de confidencialidad (GAF-CBS-FM005) y las Disposiciones de Seguridad de la Información para Proveedores, como aceptación de las mencionadas disposiciones.

7.14.2 Los proveedores sólo deben desarrollar para la entidad, aquellas actividades cubiertas bajo el correspondiente contrato u orden de servicio.

7.14.3 ***Todo proveedor que necesite más información que la acordada para cumplir su tarea, el propietario de la información, en conjunto con el Oficial de Seguridad y Confianza Digital, deberán analizar las necesidades de acceso, la factibilidad y la correspondencia entre lo solicitado y la tarea enmendada antes de entregar lo solicitado por el proveedor.***

7.14.4 Todo proveedor debe velar que su personal, que presta los servicios directamente a la entidad, cumpla con los lineamientos de seguridad de la información recogidos en la presente directiva. En caso de incumplimiento, la entidad se reserva el derecho de solicitar al proveedor el cambio de personal, sin perjuicio del derecho de resolver el contrato de prestación de servicios en los términos establecidos en el contrato.

7.14.5 El proveedor debe garantizar que todo su personal cuente con formación y capacitación apropiada para el desarrollo del servicio contratado, tanto a nivel específico en las materias correspondiente a la actividad asociada, como de manera transversal en materia de seguridad de la información.

7.14.6 Cualquier tipo de intercambio de información que se produzca entre la entidad y el proveedor se entenderá que se ha realizado dentro del marco establecido por el contrato, de modo que dicha información tendrá el carácter de confidencial y no podrá ser utilizada en ningún caso para fines diferentes a los asociados al contrato.

7.14.7 En el caso que el proveedor subcontrate a un tercero para la ejecución de un servicio, es responsable de propagar los requisitos de seguridad de la SUNASS al tercero subcontratado.

7.14.8 La entidad puede realizar auditorías para verificar que el proveedor cumple con los requisitos de seguridad establecidos, para ello, el Oficial de Seguridad y Confianza Digital planifica las auditorías en un cronograma.

7.14.9 La entidad debe realizar una verificación del impacto derivado de un cambio en el alcance del servicio del proveedor o del propio proveedor, y llevar a cabo una reevaluación integral de los riesgos asociados.

7.14.10 ***El acceso de terceros al sistema y a la de red de la institución se otorgará únicamente después de la firma del contrato y se debe definir los términos de conexión, a fin de resguardar al máximo la información de la institución. Se debe generar registros de cada acceso interno o externo. Corresponde a SUNASS especificar estándares para la conectividad remota de manera de salvaguardar la Confidencialidad, integridad y disponibilidad de la información.***

7.14.11 ***El área de Soporte Técnico es la encargada de controlar el acceso a terceros por medio de controles de acceso, que depende de la finalidad de la prestación del servicio o de una visita programada (Control de Visitas – formato).***

7.14.12 ***Todos los proveedores contratados que necesiten acceder al Datacenter deberán de registrarse en la Bitácora correspondiente y debe estar siempre acompañado por el personal de Infraestructura Tecnológica.***

7.14.13 ***Cuando el contrato implique la adquisición de una solución tecnológica o un servicio que, en parte, dependa de una solución para procesar datos personales, la adquisición debe evaluarse con respecto a las normas vigentes de protección de datos personales, para determinar el nivel asociado de riesgo.***

7.14.14 ***Los proveedores externos deben contar con procedimientos adecuados de gestión de incidentes de seguridad, que corresponde al nivel de servicio que brindan, la sensibilidad de los datos y los requisitos de la norma de protección de datos. Se debe exigir a los proveedores externos la notificación de cualquier incidente de seguridad importante tan pronto ocurra.***

7.14.15 ***El incumplimiento de los lineamientos podría resultar en la eliminación inmediata del acceso a la plataforma o a la suspensión/rescisión de los acuerdos contractuales.***

7.15 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Para garantizar un enfoque consistente para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades de la seguridad de la información, se establece lo siguiente:

7.15.1 La gestión de incidentes se realiza según lo establecido en la caracterización del proceso "Atención de eventos y debilidades de las tecnologías de la información y comunicaciones (GTI-AED-CR-N2)" y en el instructivo "Atención de eventos y debilidades de seguridad de la información (GTI-OTI-IN001)", así como, de otras disposiciones que establezca la OTI para tal fin.

7.15.2 Todo el personal, proveedor o tercero debe comunicar las debilidades y eventos identificados a la Mesa de Ayuda de la OTI (mesadeayuda@SUNASS.gob.pe); cuando se traten de debilidades o eventos de seguridad de la información, el personal de la Mesa de Ayuda de la OTI debe comunicarlo al Oficial de Seguridad y Confianza Digital, a fin de que se realicen las acciones necesarias.

7.15.3 Todo evento de seguridad de la información es registrado, clasificado, evaluado y atendido, con el fin de brindar una solución temporal o establecer una solución definitiva.

7.15.4 Los incidentes de seguridad de la información son atendidos de acuerdo con su nivel de prioridad, el cual se determina según lo señalado en el anexo 1 del presente documento.

7.15.5 El Oficial de Seguridad y Confianza Digital debe registrar las lecciones aprendidas, con el fin de generar una fuente de conocimiento en base a incidentes ya presentados y así establecer soluciones a futuros incidentes.

7.15.6 Se deben establecer acciones para la identificación, recolección y conservación de la información que puede servir como evidencia para propósitos de acción disciplinaria y legal.

7.16 SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Para proteger la confidencialidad, integridad y disponibilidad de la información ante situaciones adversas, se establece lo siguiente:

7.16.1 Son requisitos de seguridad para la continuidad del negocio:

a) Para mantener los controles de acceso a la infraestructura, se debe verificar periódicamente el cumplimiento de los lineamientos de control de acceso descritos en el numeral 7.6 de la presente directiva.
b) Contar con respaldos de la información y realizar pruebas, se debe realizar periódicamente *backups* de la información, del software y de imágenes del sistema de acuerdo con lo establecido en la caracterización del proceso "Respaldo y restauración de la información (GTI-RRI-CR-N2)" y en el instructivo "Ejecución de respaldo y restauración de la información (GTI-OTI-IN002)".

c) Contar con credenciales de accesos a los sistemas (personal autorizado), dando cumplimiento de los lineamientos de control de acceso descritos en el numeral 7.6 de la presente directiva.

7.16.2 Respecto a la implementación y verificación de los requisitos de seguridad para la continuidad del negocio:

a) El Oficial de Seguridad y Confianza Digital es el responsable de asegurar que los requisitos se encuentren implementados.
b) Los/as dueños/as de procesos deben participar en las actividades que se les solicite para la implementación, mantenimiento y asegurar que se cumplan los requisitos de seguridad definidos.
c) El Oficial de Seguridad y Confianza Digital debe asegurar que se verifica la implementación de los requisitos de seguridad de la información para la continuidad del negocio al menos una vez al año, para asegurar su validez y efectividad ante situaciones adversas; así como, elaborar un checklist de verificación de controles de seguridad y un informe del resultado de la verificación.
d) Se cuenta con infraestructura tecnológica de procesamiento de información redundante con capacidad suficiente para garantizar la disponibilidad de los servicios de TI.

7.17 CUMPLIMIENTO

Para asegurar el cumplimiento de las normas u obligaciones contractuales y de los requisitos de seguridad de la información implementados por la SUNASS, se establece que:

- La OAJ remite al Oficial de Seguridad y Confianza Digital las nuevas normas o leyes relacionadas con la seguridad de la información que le son aplicables a la entidad, las cuales son registradas o actualizadas en la "Matriz de Documentos Externos del SGSI".
- El Oficial de Seguridad y Confianza Digital debe revisar las normas y leyes relacionadas con la seguridad de la información para velar por su cumplimiento; para ello, debe coordinar con el/la directora/a o Jefe/a de la unidad de organización involucrada con la finalidad de identificar los documentos, prácticas y otros que dan cumplimiento a las nuevas exigencias normativas registradas.
- El Oficial de Seguridad y Confianza Digital debe supervisar el cumplimiento del uso de productos registrados de software y los respectivos acuerdos contractuales relacionados a los derechos de propiedad intelectual.
- La OTI cumple con el resguardo de los registros de *backups* según lo establecido en la caracterización del proceso "Respaldo y restauración de la información (GTI-RRI-CR-N2)", con ello se garantiza la confidencialidad y disponibilidad de la información que se emplea para la operatividad de los procesos de la SUNASS.
- Todo el personal debe conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan acceso con motivo del ejercicio de sus funciones, para ello, suscriben "Acuerdos de Confidencialidad". Mediante estos acuerdos comprometen a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del responsable del activo de que se trate.
- El/la Coordinador/a General del SIG debe revisar la programación de las auditorías del SGSI en coordinación con el Oficial de Seguridad y Confianza Digital establecidas en el "Programa Anual de Auditorias del SIG", como mínimo una vez al año, para asegurar su aplicabilidad; así como, realiza el seguimiento de su ejecución según lo programado. Las auditorías permiten evaluar la efectividad de los controles implementados para el SGSI.
- Los/as Directores/as y Jefes/as de cada unidad de organización de la SUNASS, deben supervisar el cumplimiento de los documentos de gestión interna (directivas, procedimientos, caracterizaciones, entre otros) relacionados a seguridad de la información, con periodicidad semestral. Los incumplimientos detectados, se registran como no conformidades y su tratamiento se realiza de acuerdo a lo establecido en

la caracterización del proceso "Observaciones, No Conformidades y Acciones Correctivas para la Mejora del Sistema Integrado de Gestión (GDI-NCA-CR-N3)".

- El Oficial de Seguridad y Confianza Digital debe revisar que anualmente se realice el análisis de vulnerabilidades de los sistemas de información en uso y de la infraestructura tecnológica, para verificar el cumplimiento de los controles técnicos implementados. El resultado de estas evaluaciones es revisado para la toma de acciones inmediatas que permitan atender las brechas y riesgos identificados.

8. ANEXOS

- Niveles de priorización para la atención de incidentes de seguridad de la información

ANEXO: NIVELES DE PRIORIZACIÓN PARA LA ATENCIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Los incidentes de seguridad de la información se priorizan en base a los criterios de impacto y criticidad de estos.

1. **Sobre el cálculo del impacto**
   Se debe considerar el impacto actual y el impacto futuro:

   IMPACTO ACTUAL: Depende de la cantidad de daño que ha provocado (puede haber sido provocado por diversos factores, como errores humanos, fallas técnicas, ataques cibernéticos o eventos naturales) en los procesos de la SUNASS, usuarios y recursos el incidente en el momento de ser detectado.

   IMPACTO FUTURO: Depende de la cantidad de daño que pueda causar el incidente en la SUNASS, usuarios y recursos si no es contenido, ni erradicado.

IMPACTO ACTUAL / IMPACTO FUTURO		
VALOR	ESCALA	DESCRIPCION
5	Crítico	Afectación en las funciones críticas del negocio por indisponibilidad o degradación excesiva del desempeño de las aplicaciones y/o servicios.
4	Mayor	Afectación en alguna de las funciones de la entidad por indisponibilidad o degradación de desempeño en las aplicaciones y/o servicios.
3	Moderado	Afectación en alguna de las funciones de la entidad o por degradación leve del desempeño de las aplicaciones y/o servicios. El incidente implica un número considerado de usuarios o partes externas afectadas.
2	Menor	Afectación en alguna de las funciones de la entidad o por degradación muy leve del desempeño de las aplicaciones y/o servicios. El incidente implica un número reducido de usuarios o partes externas afectadas y es de poca visibilidad.
1	Insignificante	Afectación en las funciones no críticas de la entidad y el usuario puede esperar una fecha determinada para la solución. El usuario puede continuar con sus tareas críticas de la operación, se mantiene la funcionalidad y el desempeño de las aplicaciones y servicios.

2. **Sobre el cálculo de la criticidad**
   Se debe considerar lo siguiente:

   CRITICIDAD: Depende del activo involucrado en la incidencia de seguridad de la información y/o nivel de operatividad del servicio requerido para la continuación de las operaciones.

CRITICIDAD		
VALOR	ESCALA	DESCRIPCION
5	Crítico	Sistemas que son de misión crítica para los procesos de la entidad.
4	Mayor	Sistemas, servicio o infraestructura crítica para la entidad.
3	Moderado	Sistemas, servicio o infraestructura considerados no crítica para la entidad.
2	Menor	Número considerable de recursos tecnológicos
1	Insignificante	Pequeño número de recursos tecnológicos.

3. Sobre la determinación de la prioridad

Se debe considerar lo siguiente:

PRIORIZACIÓN: Se procede a catalogar el incidente de seguridad de la información, basado en la determinación del nivel de impacto y criticidad, para su cálculo se requiere de la siguiente fórmula:

Criticidad general = (Valuación impacto actual * 0.25) + (Valuación impacto futuro * 0.25) + (valuación de la criticidad * 0.5)

Con el resultado anterior se indica el nivel de prioridad para su atención de la siguiente manera:

PRIORIZACION		
RANGO	ESCALA	TIEMPO DE RESPUESTA
3.75 a 5.00	Crítica	Inmediato
2.50 a 3.74	Alta	3 horas
1.88 a 2.49	Media	8 horas
1.25 a 1.87	Baja	24 horas
0.00 a 1.24	Mínima	48 horas

En base al resultado de la evaluación del nivel de prioridad del incidente se indica su valoración de la siguiente manera:

- Crítica: Si afecta al desenvolvimiento del trabajo de los usuarios y el funcionamiento de la entidad no puede esperar.
- Alta: Si afecta al desenvolvimiento del trabajo de los usuarios y el funcionamiento de la entidad puede esperar hasta 3 horas para su atención.
- Media: Si afecta al desenvolvimiento del trabajo de los usuarios y el funcionamiento de la entidad puede esperar hasta 8 horas para su atención.
- Baja: Si afecta al desenvolvimiento del trabajo de los usuarios y el funcionamiento de la entidad puede esperar hasta 24 horas para su atención.
- Mínima: Si afecta al desenvolvimiento del trabajo de los usuarios y el funcionamiento de la entidad puede esperar hasta 48 para su atención.