LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD DE LA INFORMACIÓN

ROL	NOMBRE	CARGO
Modificado por:	Jenny Castañeda Zubiaur	Oficial de Seguridad y Confianza Digital
Revisado por:	Gustavo Adolfo Bernal Soto	Jefe 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	GENERAL	• Se modificó la estructura del numeral "7. DIPOSICIONES ESPECIFICAS", con el propósito de organizar el desarrollo de los lineamientos establecidos por la Sunass para el Sistema de Gestión de Seguridad de la Información, conforme a lo señalado en el Anexo A de la norma ISO/IEC 27001:2022. El contenido de este numeral fue reorganizado, pasando de 17 numerales a 4: - 7.1 Controles Organizacionales. - 7.2 Controles de Personal - 7.3 Controles Físicos - 7.4 Controles Tecnológicos • Se incorporó la referencia correspondiente a los controles del Anexo A de la norma ISO/IEC 27001:2022 en cada lineamiento establecido en la presente directiva. • Se reemplazo la denominación "Mesa de Ayuda" por el "Sistema de Mesa de Servicios" en toda la directiva. • Se modificó la numeración como consecuencia de las modificaciones realizadas y se eliminaron diversos lineamientos que ya no resultan aplicables bajo el contexto de la norma ISO/IEC 27001:2022. • Se eliminó el Anexo "Niveles de Priorización para la Atención de Incidentes de Seguridad de la Información", por no corresponder a lineamientos, sino a especificaciones operativas del proceso de "Atención de eventos, incidentes y debilidades de seguridad de la información"; estas especificaciones serán incluirán en su respectivo instructivo.
2	2. BASE NORMATIVA	• Se reemplazó la *"Norma Técnica Peruana NTP – ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Seguridad de la Información. Requisitos"* por *"Resolución Directoral N.º 022-2022-INACAL/DN, se aprueba la actualización de la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3a Edición"*, por ser la versión vigente. • Se incorporaron las normas: "Resolución Directoral N.º 022-2022-INACAL/DN, se aprueba la actualización de la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3a Edición" y la "Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM-SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información".
3	4. SIGLAS/ ACRÓNIMOS	• Se incorporaron las siglas CNSD y OSCD, y se empleó en todo el documento.
4	5. DEFINICIONES	• Se incorporaron las definiciones "Dispositivo de punto final de usuario", "Disrupción", "Información confidencial", "Información de identificación personal (IIP)", "Instalación de procesamiento de información" y "Tercero".
5	6. DISPOSICIONES GENERALES	• En el numeral 6.3, se incorporó el texto "establecidos en la presente directiva" para precisarlo. • En el numeral 6.4, se reemplazó "Sunass" por la expresión "La alta dirección y los responsables de las unidades de organización" para precisarlo.
6	7.1 CONTROLES ORGANIZACIONALES	• Se incorporaron los numerales 7.1.5, 7.1.15, 7.1.18, 7.1.20, 7.1.21, 7.1.23, 7.1.24, 7.1.26 y 7.1.28, para establecer lineamientos vinculados a los controles A.5.7, A.5.17, A.5.20, A.5.22, A.5.23, A.5.29, A.5.30, A.5.32 y A.5.34 del Anexo A de la norma ISO/IEC 27001:2022, respectivamente. • Numeral 7.1.4 (antes 7.1.3), relacionado a los controles A.5.5 y A.5.6, se reemplazó su contenido para precisar la responsabilidad del/ de la Oficial de Seguridad y Confianza Digital. • Numeral 7.1.6 (antes 7.1.4), relacionado con el control A.5.8, se modificó para precisar como se integra la seguridad de la información en la gestión de proyectos. • Numeral 7.1.7, relacionado con el control A.5.9 - Se modificó el literal a) tomando como base los literales a) y b) del numeral 7.5.1 de la versión anterior, con el fin de precisar la responsabilidad de los/as dueños/as de los procesos y de la OTI respecto al inventario de activos de información. - Se incorporó el literal b) como nuevo lineamiento.

N°	Ítems (Sección del documento)	Descripción del cambio (*)
		• Numeral 7.1.8, relacionado con el control A.5.10 - Se reubicó el contenido del literal c) del numeral 7.5.1 de la versión anterior, eliminando los puntos que no se alineaban con el control establecido en este apartado y reorganizando el contenido en literales. - Se modificaron los literales b) y e) para precisar su redacción. - Se incorporaron los literales a), c) y d) como nuevos lineamientos. • En el numeral 7.1.9, relacionado con el control A.5.11, se reubicó el contenido del literal d) del numeral 7.5.1 de la versión anterior, para estar alineado con el control establecido en este apartado. • Numeral 7.1.10, relacionado con el control A.5.12 - Se reubicó el contenido del literal a) del numeral 7.5.2 de la versión anterior y se reorganizó en literales. - Se modificó el literal b), sobre el "uso interno", agregando las expresiones "con la autorización del propietario del activo y" y "Toda información que no ha sido clasificada específicamente debe ser tratada como de uso interno", para precisarlo. • Numeral 7.1.11, relacionado con el control A.5.13 - Se reubicó el contenido del literal b) del numeral 7.5.2 de la versión anterior, eliminando los puntos que no se alineaban con el control establecido en este apartado y reorganizando el contenido en literales. - El literal b) fue trasladado desde el cuarto punto del literal c) del numeral 7.5.2 de la versión anterior. • Numeral 7.1.12, relacionado con el control A.5.14 - Se reubicó el contenido del numeral 7.11.2 de la versión anterior, eliminando los literales que no se alineaban con el control establecido en este apartado. - Se modificó el literal b) (antes literal d), para precisar como se realiza la transferencia o intercambio de información con entidades externas. - El literal c) fue trasladado desde el tercer punto del literal b) del numeral 7.5.2 de la versión anterior, y se modificó para precisar su contenido. - Se modificó el literal d) (antes literal i), para precisar la responsabilidad de los usuarios respecto a su cuenta de correo electrónico institucional. - El literal e) fue trasladado desde el tercer punto del literal c) del numeral 7.5.1 de la versión anterior. - El literal f) y g) fueron trasladados desde el segundo punto del literal c) y del cuarto punto del literal b) del numeral 7.5.2 de la versión anterior, respectivamente. - Se incorporó el literal h) como nuevo lineamiento. • En el numeral 7.1.13, relacionado con el control A.5.15, se reubicó y reemplazó el contenido del numeral 7.6 de la versión anterior para alinearlo con el control establecido en este apartado. • Numeral 7.1.14, relacionado con el control A.5.16 - Se incorporaron los literales a), c), d), e), f) y g) como nuevos lineamientos. - El literal b) fue trasladado desde el literal b) del numeral 7.6.4 de la versión anterior y modificado para precisar como se debe solicitar la creación de usuarios genéricos. • Numeral 7.1.16, relacionado con el control A.5.18 - Se reubicó el contenido del numeral 7.6.4 de la versión anterior, eliminando los literales que no se alineaban con el control establecido en este apartado. - Se modificaron los literales b), c) y d) (antes literales e), f) y k), respectivamente), para precisar su contenido. - Se incorporó el literal a) como nuevo lineamiento. • Numeral 7.1.17, relacionado con el control A.5.19. - El literal a) y b) fueron trasladados desde el numeral 7.14.1 y 7.14.4 de la versión anterior, respectivamente, y modificados para precisar la responsabilidad del proveedor. - Se incorporó el literal c) como nuevo lineamiento.

N°	Ítems (Sección del documento)	Descripción del cambio (*)
		• En el numeral 7.1.19, relacionado con el control A.5.21, se reubicó el contenido del numeral 7.14.7 de la versión anterior para alinearlo con el control establecido en este apartado. • Numeral 7.1.22 (antes 7.15), relacionado con el control A.5.24 - Se incorporó el literal a) como nuevo lineamiento. - El literal b) fue traslado desde el numeral 7.15.1 de la versión anterior. - Se eliminaron los numerales 7.15.3, 7.15.4, 7.15.5 y 7.16.6, por no estar alineados con el control establecido en este apartado. • Numeral 7.1.25 (antes 7.17), relacionado con el control A.5.31 - El literal a) fue trasladado desde el primer punto del numeral 7.17 de la versión anterior. - El literal b) fue trasladado desde el segundo punto del numeral 7.17 de la versión anterior y modificado para precisar la responsabilidad del/ de la Oficial de Seguridad y Confianza Digital, en relación con la coordinación del cumplimiento normativo. • En el numeral 7.1.27, relacionado con el control A.5.33, se reubicó el contenido del cuarto punto del numeral 7.17 de la versión anterior para alinearlo con el control establecido en este apartado y se modificó para precisar el tipo de registros que se protegen. • Los numerales 7.1.29, 7.1.30 y 7.1.31, relacionados con los controles A.5.35, A.5.36 y A.5.37, fueron trasladados desde el sexto y séptimo punto del numeral 7.17 y del numeral 7.10.2 de la versión anterior, respectivamente, por estar alineados con el control establecido en este apartado.
7	7.2 CONTROLES DE PERSONAL	• Numeral 7.2.1, relacionado al control A.6.1 Los literales a) y b) fueron trasladados desde el numeral 7.4.1 de la versión anterior, por estar alineados con el control establecido en este apartado. • Numeral 7.2.2, relacionado con el control A.6.2 - El literal a) fue trasladado desde el literal d) del numeral 7.4.1 de la versión anterior y modificado para precisar donde se establecen las funciones, responsabilidades y funciones del personal de la Sunass. - El literal b) fue trasladado desde el literal g) del numeral 7.4.1 de la versión anterior, por estar alineado con el control establecido en este apartado. • En el numeral 7.2.3, relacionado con el control A.6.3, se reubicó el contenido del literal a) del numeral 7.4.2 de la versión anterior, eliminando el último punto por no estar alineado con el control establecido en este apartado. . • En el numeral 7.2.4, relacionado con el control A.6.4, se reubicó el contenido del literal b) del numeral 7.4.2 de la versión anterior, por estar alineado con el control establecido en este apartado. • Numeral 7.2.5 (antes 7.4.3), relacionado con el control A.6.5 - Se reubicó el contenido de los literal a), b) y c) del numeral 7.4.3 de la versión anterior en los literales b), c) y d) de este apartado. - Se incorporó el literal a) como nuevo lineamiento. - Se eliminó el literal d) del numeral 7.4.3 de la versión anterior de esta directiva, por no estar alineado con el control establecido en este apartado. • Numeral 7.2.6, relacionado con el control A.6.6 - El literal a) fue trasladado desde el literal f) del numeral 7.4.1 de la versión anterior, por estar alineado con el control establecido en este apartado. - Se incorporó el literal b) como nuevo lineamiento. • Numeral 7.2.7 (antes 7.3), relacionado con el control A.6.7 - El literal a) fue trasladado desde el primer párrafo del numeral 7.3 de la versión anterior, por estar alineado con el control establecido en este apartado.

N°	Ítems (Sección del documento)	Descripción del cambio (*)
		- En el literal b) fueron trasladados el quinto, séptimo y decimo punto del literal a) del numeral 7.3.1 de la versión anterior, así como los literales c) y d) del dicho numeral. Además, se incorporaron los incisos i e ii para establecer nuevas responsabilidades al personal en modalidad de teletrabajo. - En el literal c) fueron trasladados los literales c), d), f) e i) del numeral 7.3.2 de la versión anterior con algunas modificaciones de forma. • Numeral 7.2.8, relacionado con el control A.6.8 - El literal a) fue trasladado desde el numeral 7.15.2 de la versión anterior, por estar alineado con el control establecido en este apartado - El literal b) fue trasladado desde el literal d) del numeral 7.10.11 de la versión anterior y modificado para precisar su contenido.
8	7.3 CONTROLES TECNOLÓGICOS	• Se incorporaron los numerales 7.3.1, 7.3.3, 7.3.4 y 7.3.5 para establecer lineamientos vinculados a los controles A del Anexo A.7.1, A.7.3, A.7.4 y A.7.5 de la norma ISO/IEC 27001:2022, respectivamente. • En el numeral 7.3.2, relacionado con el control A.7.2, se reubicó el contenido del literal e) del numeral 7.8.1 de la versión anterior y se modificó para precisarlo. • Numeral 7.3.6, relacionado con el control A.7.6 - Se incorporaron los literales a) y b) como nuevos lineamientos. - Los literales c) y d) fueron trasladados desde el literal g) y el segundo punto del literal f) del numeral 7.8.1 de la versión anterior, respectivamente, por estar alineados con el control establecido en este apartado. • Numeral 7.3.7, relacionado con el control A.7.7 - El literal a) fue traslado desde el numeral 7.9.3 de la versión anterior, con la modificación del tiempo de bloqueo automático de los equipos de 15 a 5 minutos. - Los literales b), c) y d) fueron trasladados desde el numeral 7.9.4 de la versión anterior, por estar alineados con el control establecido en este apartado. - Los literales e) y f) fueron trasladados desde los literales b) y d) del numeral 7.9.5 de la versión anterior, por estar alineados con el control establecido en este apartado. • Numeral 7.3.8, relacionado con el control A.7.8 - El literal a) fue trasladado desde los numerales 7.9.1 y 7.9.2 de la versión anterior y modificado para precisarlo. - Los literales b), c), d) y e) fueron trasladado desde los puntos que conforman el literal a) del numeral 7.8.2 de la versión anterior, eliminando el primer punto por no estar alineado con el control establecido en este apartado. • Numeral 7.3.9, relacionado con el control A.7.9 - El literal a) fue trasladado desde el literal d) del numeral 7.8.2 de la versión anterior, por estar alineado con el control establecido en este apartado. - El literal b) fue trasladado desde el literal e) del numeral 7.8.2 de la versión anterior y modificado para precisar como se protegen los equipos de propiedad de la Sunass. • Numeral 7.3.10, relacionado con el control A.7.10 - Se incorporaron los literales a), b) y f) como nuevos lineamientos. - Los literales c) y d) fueron trasladados desde los literales e) y d) del numeral 7.5.3 de la versión anterior y modificados para precisar el manejo de los medios de almacenamiento. - El literal e) fue trasladado desde el tercer punto del literal c) del numeral 7.5.2 de la versión anterior, por estar alineado con el control establecido en este apartado. • Numeral 7.3.11, relacionado con el control A.7.12 Los literales a) y b) fueron trasladado desde el segundo y tercer punto del literal b) del numeral 7.8.2 de la versión anterior. Se preciso en el literal b) que la responsabilidad corresponde a la OTI.

N°	Ítems (Sección del documento)	Descripción del cambio (*)
		• En el numeral 7.3.12, relacionado con el control A.7.13, se reubicó el contenido del literal c) del numeral 7.8.2 de la versión anterior para alinearlo con el control establecido en este apartado. • En el numeral 7.3.13, relacionado con el control A.7.14, se reubicó el contenido del literal f) del numeral 7.5.3 de la versión anterior y se modificó para precisar su contenido.
9	7.4 CONTROLES TECNOLOGICOS	• Se incorporaron los numerales 7.4.5, 7.4.9, 7.4.11, 7.4.12 y 7.4.26, para establecer lineamientos vinculados a los controles A del Anexo A.8.5, A.8.9, A.8.11, A.8.12 y A.8.28 de la norma ISO/IEC 27001:2022, respectivamente. • Numeral 7.4.1, relacionado con el control A.8.1 - El literal b) fue trasladado desde el literal g) del numeral 7.2.7 de la versión anterior y se modificó su contenido - Los literales c), d) y q) fueron trasladados desde los numerales 7.2.2, 7.2.3 y 7.2.8 de la versión anterior, respectivamente y se modificó su contenido. - Los literales e) y l) fueron trasladados desde los literales f) y a) del numeral 7.2.7 de la versión anterior, respectivamente, y se modificó su contenido. - Se incorporaron los literales a), f), g) h), i). j), k), m), n), o) y p) como nuevos lineamientos. • Numeral 7.4.2, relacionado con el control A.8.2 - Los literales a), b), c), d), e) y f) fueron trasladados desde el literal i) del numeral 7.6.4 de la versión anterior y se eliminaron los puntos que no se encontraban alineados con el control establecido en este apartado y se modificó la redacción para precisar su contenido. - El literal g) fue trasladado desde el literal d) del numeral 7.10.1 de la versión anterior y se modificó para precisar su contenido. - Se incorporó el literal h) como nuevo lineamiento. • En el numeral 7.4.3, relacionado con el control A.8.3, se reubicó el contenido de los literales a) y h) del numeral 7.6.6 de la versión anterior en los literales a) y b) por estar alineados con el control establecido en este apartado. Se modificó la redacción del literal a) para precisar los controles que aplica la OTI para restringir el acceso a la información. • En el numeral 7.4.4, relacionado con el control A.8.4, se reubicó el contenido del literal f) del numeral 7.6.6 de la versión anterior, por estar alineado con el control establecido en este apartado y se modificó para precisar que la OTI es responsable de controlar el acceso al código fuente. • En el numeral 7.4.6, relacionado con el control A.8.6, se reubicó el contenido del numeral 7.10.4 de la versión anterior por estar alineado con el control establecido en este apartado, y se modificó para precisar que la OTI es responsable de gestionar la capacidad de las TIC. • Numeral 7.4.7, relacionado con el control A.8.7 - Se reubicó el contenido del numeral 7.10.6 de la versión anterior, por estar alineado con el control establecido en este apartado, eliminando su literal b). - El literal f) fue trasladado desde el literal b) del numeral 7.10.1 de la versión anterior y se precisó como una prohibición para el usuario. • Numeral 7.4.8, relacionado con el control A.8.8 - Se reubicó el contenido del numeral 7.10.10 de la versión anterior, por estar alineado con el control establecido en este apartado, eliminando su literal f). - En el literal a) se incorporó una precisión final, indicando que los hallazgos y recomendaciones del análisis de vulnerabilidades deben ser evaluados e implementados, cuando corresponda. • Numeral 7.4.10, relacionado con el control A.8.10 - Se incorporó el literal a) como nuevo lineamiento.

N°	Ítems (Sección del documento)	Descripción del cambio (*)
		- Los literales b) y c) fueron trasladados desde el literal l) del numeral 7.6.4 y del literal i) del numeral 7.5.3 de la versión anterior, respectivamente, por estar alineado con el control establecido en este apartado. • Numeral 7.4.13, relacionado con el control A.8.13 - Se reubicó el contenido del numeral 7.10.7 de la versión anterior, por estar alineado con el control establecido en este apartado. - Se modificó el literal b) para precisar la responsabilidad de la OTI respecto al respaldo y las pruebas de recuperación de la información. • En el numeral 7.4.14, relacionado con el control A.8.14, se reubicó el contenido del literal d) numeral 7.16.2 de la versión anterior, por estar alineado con el control establecido en este apartado, y se modificó para precisar la responsabilidad de la OTI sobre la infraestructura tecnológica. • Numeral 7.4.15, relacionado con el control A.8.15 - Los literales a) y b) fueron trasladados desde el literal b) y c) del numeral 7.10.8 de la versión anterior, por estar alineados con el control establecido en este apartado. - El literal c) fue trasladado desde el literal e) del numeral 7.10.11 de la versión anterior, por estar alineado con el control establecido en este apartado - El literal d) fue trasladado desde el literal c) del numeral 7.10.1 de la versión anterior y se precisó como prohibición. • Numeral 7.4.16, relacionado con el control A.8.16 - Se incorporaron los literales a) y b) como nuevos lineamientos - El literal c) fue trasladado desde el literal e) del numeral 7.11.2 de la versión anterior, por estar alineado con el control establecido en este apartado • En el numeral 7.4.17, relacionado con el control A.8.17, se reubicó el contenido del literal d) numeral 7.10.8 de la versión anterior, por estar alineado con el control establecido en este apartado, y se modificó para precisar la responsabilidad de la OTI. • En el numeral 7.4.18, relacionado con el control A.8.18, se reubicó el contenido de los literales c), d) y e) del numeral 7.6.6 de la versión anterior, por estar alineado con el control establecido en este apartado. • Numeral 7.4.19, relacionado con el control A.8.19 - Se incorporó el literal a) como nuevo lineamiento. - Se reubicó el contenido del numeral 7.10.9 de la versión anterior, por estar alineado con el control establecido en este apartado, eliminando los literales a) y e). - Se modificó el literal b) para precisar la prohibición del uso de software o programas ilegales, sin licencia, piratas o de su propiedad. • Numeral 7.4.20, relacionado con los controles A.8.20, A.8.21 y A.8.22 - Se reubicó el contenido del numeral 7.11.1 de la versión anterior, por estar alineado con el control establecido en este apartado. - El literal l) fue trasladado desde el literal e) del numeral 7.2.6 de la versión anterior, por estar alineado con el control establecido en este apartado. • Numeral 7.4.21, relacionado con el control A.8.23 - Se incorporaron los literales a) y b) como nuevos lineamientos, - El literal c) fue trasladado desde el literal e) del numeral 7.10.4 de la versión anterior, por estar alineado con el control establecido en este apartado. • En el numeral 7.4.22, relacionado con el control A.8.24, se reubicó el contenido del numeral 7.7 de la versión anterior, por estar alineado con el control establecido en este apartado, eliminando la expresión "Se debe emplear un listado de software NO autorizado (lista negra) para evitar su uso o un listado de software autorizado (lista blanca)".

N°	Ítems (Sección del documento)	Descripción del cambio (*)
		• En el numeral 7.4.23, relacionado con el control A.8.25, se reubicó el contenido del numeral 7.13 de la versión anterior, por estar alineado con el control establecido en este apartado, eliminando los literales b), d), i), o) y p). • Numeral 7.4.24, relacionado con el control A.8.26 - Se reubicó el contenido del numeral 7.12.4 de la versión anterior, por estar alineado con el control establecido en este apartado. - Los literales a) y b) fueron trasladados desde el literal c) y d) del numeral 7.12.1 versión anterior, por estar alineado con el control establecido en este apartado. • Numeral 7.4.25, relacionado con el control A.8.27 - Los literales a) y b) fueron trasladados desde el literal e) del numeral 7.12.2 de la versión anterior, por estar alineado con el control establecido en este apartado. - Los literales c) al h) fueron trasladados desde el literal a) del numeral 7.12.2 de la versión anterior, por estar alineados con el control establecido en este apartado. • En los numerales 7.4.27 y 7.4.28, relacionados con los controles A.8.29 y A.8.30, se reubicó el contenido de los literales h) y g) del numeral 7.12.2 de la versión anterior, por estar alineados con los controles establecidos en cada apartado. • En el numeral 7.4.29, relacionado con el control A.8.31, se reubicó el contenido de los literales b) y f) del numeral 7.12.2 de la versión anterior, por estar alineado con el control establecido en este apartado. • Numeral 7.4.30, relacionado con el control A.8.32 - Se reubicó el contenido del numeral 7.10.3 de la versión anterior, por estar alineado con el control establecido en este apartado. - Los literales a) y b) fueron trasladados desde los literales c) y d) del numeral 7.12.2 de la versión anterior, por estar alineados con el control establecido en este apartado. • En el numeral 7.4.31, relacionado con el control A.8.33, se reubicó el contenido del numeral 7.12.3 de la versión anterior, por estar alineado con el control establecido en este apartado. • Numeral 7.4.32, relacionado con el control A.8.34 Los literales a), b) y c) fueron trasladados desde el numeral 7.10.11 de la versión anterior, por estar alineados con el control establecido en este apartado.

(*) 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. Ley N.º 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.

3.5. 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.

3.6. Decreto Supremo Nº 157-2021-PCM, aprueba el Reglamento del Decreto de Urgencia N.º 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.

3.7. Resolución Directoral N.º 022-2022-INACAL/DN, se aprueba la actualización de la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3a Edición.

3.8. Resolución de Secretaría de Gobierno y Transformación Digital N.º 002-2023-PCM-SGTD, que aprueba la Directiva N.º 001-2023-PCM/SGTD, Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital.

3.9. Resolución de Secretaría de Gobierno y Transformación Digital N.º 003-2023-PCM-SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información.

4. SIGLAS / ACRONIMOS

CNSD ***: Centro Nacional de Seguridad Digital de la PCM***
OAJ : Oficina de Asesoría Jurídica
OTI : Oficina de Tecnologías de la Información
OSCD ***: Oficial de Seguridad y Confianza Digital***
RISS : Reglamento Interno de Servidores Civiles de la Sunass.
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 la información y los activos asociados como bienes o servicios tangible o intangible, que generan, procesan o almacenan información, a los que se les 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 de punto final de usuario: Es el dispositivo de hardware de Tecnología de información y comunicaciones (TIC) conectado a la red. Puede referirse a computadoras de escritorio, laptops, teléfonos inteligentes, tablets, clientes ligeros, impresoras u otro hardware especializado, incluidos medidores inteligentes y dispositivos del Internet de las Cosas (IoT).

5.9. 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.

5.10. Disrupción: Es el incidente, previsto o no previsto, que ocasiona una desviación negativa no planificada de la entrega esperada de productos y servicios, de acuerdo con los objetivos de una organización.

5.11. Información confidencial: Es la información que no está destinada a estar disponible o ser divulgada a individuos, entidades o procesos no autorizados.

5.12. Información de identificación personal (IIP): Es cualquier información que se puede usar para identificar, contactar o localizar a una persona. Ejemplos de IIP incluyen nombre, dirección, número de teléfono, dirección de correo electrónico, número de seguro social y datos de identificación en línea como dirección IP o nombres de usuario.

5.13. Instalación de procesamiento de información: Es cualquier sistema, servicio o infraestructura de procesamiento de información, sí como la ubicación física que los alberga

5.14. 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.

5.15. 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.

5.16. Proveedor: Es la persona natural o jurídica que brinda un servicio o producto a la Sunass.

5.17. 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.

5.18. 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.

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

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

5.21. 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.

5.22. 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.

5.23. 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.

5.24. 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.

5.25. Tercero: Es toda persona que no cuenta con un vínculo laboral con la entidad, pero que requiere hacer uso de sus activos de información, ya sea para la prestación de un servicio (proveedores), en calidad de visitante o como administrado (empresa prestadora de servicios de agua potable y saneamiento o usuario del servicio de agua potable y saneamiento).

5.26. Usuario/a: Es toda persona, sea funcionario o servidor público, practicante, *tercero**, visitante u otro***, sin importar su vínculo, 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/***La OSCD*** 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 ***OSCD*** difunde los lineamientos específicos de seguridad de la información ***establecidos en la presente directiva*** para concientizar a los/as usuarios/as de la Sunass y promover su contribución a la efectividad del SGSI.

6.4. ***La alta dirección y los responsables de las unidades de organización***, en el marco de su compromiso con la seguridad de la información, monitorean la aplicación y cumplimiento de la presente directiva.

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 RIS 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. CONTROLES ORGANIZACIONALES

7.1.1. ***Roles y Responsabilidades en seguridad de la información (A.5.2)***
Los roles y responsabilidades para la seguridad de la información en la Sunass se encuentran establecidas en la GDI-MAS-IG004 Matriz de roles, responsabilidades y autoridades del SIG, que se encuentra disponible en el portal del SIG de la Sunass (intranet).

7.1.2. ***Segregación de Funciones (A.5.3)***
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. ***Responsabilidades de la dirección (A.5.4)***
Los responsables de las unidades de organización de la Sunass deben requerir que todo el personal a su cargo aplique y dé cumplimiento a lo establecido en la presente directiva.

7.1.4. ***Contacto con Autoridades y Grupos de Especiales de Interés (A.5.5 y A.5.6)***
El/La OSCD mantiene actualizada la "Lista de Contactos con Autoridades y Grupos de Interés", con el fin de hacer uso de ella ante las necesidades de comunicación o consulta sobre aspectos relacionados a la seguridad de la información y/o seguridad digital.

7.1.5. ***Inteligencia de Amenazas (A.5.7)***
La información relacionada a las amenazas a la seguridad de la información es recopilada y analizada, conforme a lo siguiente:

a) El/La OSCD recopila información proveniente de las comunicaciones y alertas de seguridad digital emitidas por el CNSD, así como de reportes externos confiables. Posteriormente, analiza dicha información y la comunica a la unidad de organización responsable del control asociado, para la ejecución de acciones de prevención, detección y/o respuesta.
b) La OTI, recopila información de las amenazas provenientes de los eventos de seguridad relacionadas con los activos críticos informáticos y proveedores de tecnologías de la

información. Posteriormente, analiza esta información y ejecuta las actividades correspondientes para su prevención, detección y/o respuesta.

c) La unidad de organización involucrada en la prevención, detección y/o respuesta de la amenaza, debe asegurar que dicha información de las amenazas sea considerada en la revisión de riesgos de seguridad de la información, y de ser el caso, debe gestionar la inclusión o actualización de los riesgos identificados.

7.1.6. ***Seguridad de la Información en la Gestión de Proyectos (A.5.8)***

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 ***(sea tecnológico o no). Por ello, el responsable de la unidad de organización encargado del proyecto debe asegurar que en su etapa inicial se realice la evaluación de riesgos de seguridad de la información y comunicar a la OSCD para el apoyo correspondiente***.

7.1.7. ***Inventario de Información y Otros Activos Asociados (A.5.9)***

a) Los/as dueños/as de los procesos que forman parte del alcance del SGSI, deben mantener actualizado el "Inventario de Activos de Información", donde se precisa al propietario y la ubicación de cada activo. Esta actividad se realiza como mínimo una vez al año o ante ***alguna*** modificación ***en las propiedades de seguridad de los activos registrados***; lo que suceda primero. ***La propiedad de los activos de información está referida a la autoridad y responsabilidad formal, sobre su identificación, clasificación, acceso, modificación y/o eliminación.***

b) La OTI es responsable de mantener un inventario de activos informáticos institucional (computadoras, portátiles, servidores, tablets, software), actualizarlo mínimamente de forma semestral. Toda adquisición de un activo informático debe tener la aprobación de la OTI. La OTI debe mantener actualizado el listado de los proveedores de activos informáticos (Software y Hardware).

7.1.8. ***Respecto al Uso Aceptable de la información y de los Activos Asociados (A.5.10)***

a) Todo usuario que tenga contacto con la información y activos asociados de Sunass debe utilizarlos y gestionarlos de manera responsable, protegiéndolos frente a accesos, modificaciones, transferencias o eliminaciones no autorizadas; ***siendo cauteloso en su manejo y teniendo presente las disposiciones normativas internas y externas en materia de seguridad de la información, protección de datos personales, confidencialidad y demás regulaciones relacionadas con la protección de datos e información.***

b) El uso o manejo de los activos de información asociados debe ***realizarse sólo para los fines establecidos por la Sunass y que se encuentren autorizadas***, de acuerdo con los lineamientos y procedimientos que se definan y considerando criterios de buen uso.

c) Todo usuario que haya sido autorizado para el uso de los servicios de internet y correo electrónico institucional debe utilizarlos exclusivamente para el cumplimiento de sus funciones u obligaciones, y no para fines personales. Asimismo, debe evitar el registro de la dirección de correo electrónico en foros, redes sociales u otros servicios externos.

d) Todo usuario debe hacer uso de las aplicaciones, sistemas, recursos y servicios informáticos de la Sunass de acuerdo con las disposiciones establecidas por la OTI, evitando el acceso a contenido indebido u ofensivo, así como la ejecución de programas desconocidos.

e) Se aplican las sanciones establecidas en el RIS de la Sunass al personal que ponga en riesgo los activos de información ***asociados***.

7.1.9. ***Devolución de Activos (A.5.11)***

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.

7.1.10. ***Clasificación de la Información (A.5.12)***

Los activos de información son clasificados y registrados en el "Inventario de Activos de Información" considerando las necesidades de confidencialidad, integridad y disponibilidad. Los activos del tipo información adicionalmente son categorizados en:

a) **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.
b) **Uso Interno:** Es la información cuyo contenido sólo es de uso y divulgación del personal de la Sunass. Sólo podrán ser divulgados a terceros ***con la autorización del propietario del activo y*** mediante la firma de un acuerdo de confidencialidad, siempre y cuando su divulgación no impacte a la entidad. ***Toda información que no ha sido clasificada específicamente debe ser tratada como de uso interno.***
c) **Público:** Es la información no sensible de acceso público y que su divulgación no genera impacto a la entidad.

7.1.11. ***Etiquetado de la Información (A.5.13)***

La información impresa y digital se etiqueta según las siguientes consideraciones:

a) 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.
b) 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).

7.1.12. ***Respecto a la Transferencia de Información (A.5.14)***

a) 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.
b) Para la transferencia ***o intercambio*** de información con entidades externas, se deben realizar acuerdos de transferencia segura ***y confidencialidad*** de la información***, usando mecanismos técnicos seguros, controles y credenciales de acceso.***
c) ***Toda transferencia*** de información clasificada como "Confidencial" debe ***realizarse*** por medios de transporte conocidos, seguros ***y confiables***.
d) Los usuarios ***que tengan asignado una cuenta de correo electrónico institucional*** deben ***evitar*** enviar, reenviar y/o responder a ***correos masivos, cadenas, anuncios o*** listas de distribución relacionadas con temas no institucionales.

e) 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.
f) 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.
g) La información con clasificación "Confidencial" que se envía por correo electrónico, debe indicar en el cuerpo del correo esta clasificación.
h) ***Los colaboradores deben evitar tener conversaciones verbales confidenciales en lugares públicos o por medios de comunicación inseguros (como mensajes de voz o contestadoras), ya que pueden ser escuchados por personas no autorizados.***

7.1.13. ***Control de Acceso (A.5.15)***

La Sunass establece controles de acceso físico y lógico para proteger los activos de información:

a) El acceso a la información debe ser coherente con su clasificación y estar en concordancia con la necesidad que tiene el usuario que requiere el acceso para realizar sus tareas, actividades, cumplir sus funciones o cual sea el objeto del vínculo con la entidad.
b) El propietario del activo de información establece las restricciones de acceso a la información, tomando en consideración el principio de mínimo privilegio. Asimismo, es responsable de autorizar el acceso de los usuarios a los activos de información de su propiedad, revisarlos semestralmente y revocar o solicitar la revocación de los accesos cuando corresponda.
c) El acceso a los recursos, aplicaciones y servicios informáticos se basan en perfiles y debe ser solicitado por el usuario a través del Sistema de Mesa de Servicios con la respectiva autorización del responsable de la unidad de organización en la que labora o prestan servicios.

7.1.14. ***Gestión de Identidades (A.5.16)***

La gestión de la identificación de los usuarios con acceso a la información es primordial para evitar comprometer la seguridad de la información. Para ello, se establece lo siguiente:

a) ***La URH es responsable de solicitar la alta y baja de las cuentas institucionales para el personal, así como comunicar sobre las rotaciones o licencias para mantener actualizadas las dependencias en los sistemas y aplicaciones informáticas.***
b) ***Los/as responsables de las unidades de organización, solo en el caso que sea estrictamente necesario podrán solicitar a través del Sistema de Mesa de Servicios,*** la creación de usuarios genéricos para servicios específicos, los mismos que son reportados al/ a la ***OSCD***. ***Los/as responsables de las unidades de organización deben solicitar la desactivación de la cuenta cuando esta no sea necesaria o se haya cumplido la necesidad.***
c) ***El personal de soporte técnico, a través de del Sistema de Mesa de Servicios atiende las solicitudes de alta y baja de cuentas institucionales de usuarios, así como cuentas institucionales para proyectos o eventos, de acuerdo con lo establecido en la caracterización del proceso "GTI-ACI-CR-N3 Administración de cuentas institucionales".***
d) ***El/La Jefe/a de la OTI es responsable de autorizar la creación de cuentas genéricas para servicios o aplicaciones, así como de revisarlas con una periodicidad mínima semestral.***
e) ***El usuario no debe hacer uso de una cuenta institucional asignada a otro usuario. En caso de incumplimiento, será considerado como suplantación de identidad***.

f) ***La firma digital asignada al personal es de uso exclusivo para el cumplimiento de sus funciones, por lo que está expresamente prohibido su uso para otros fines.***

g) ***La OTI es responsable de gestionar la identificación digital de los usuarios a los sistemas de información que se encuentren dentro de su ámbito de administración.***

7.1.15. ***Información de Autenticación (A.5.17)***

La información de autenticación para las aplicaciones, sistemas de información y servicios informáticos es la contraseña asociada a la cuenta de usuario, proyecto o servicio. Para ello, se establece lo siguiente:

a) ***El personal de soporte técnico comunica al usuario una credencial inicial que es temporal para el primer inicio de sesión y cambio de contraseña.***

b) ***Las contraseñas de los usuarios deben cumplir con las siguientes condiciones:***
   - ***i. Debe contar con una longitud de mínimo de doce (12) caracteres***
   - ***ii. Debe usar una combinación de letras en mayúscula, minúscula, números y caracteres especiales (por ejemplo: ¡, $, #, %.).***
   - ***iii. No debe de contener datos personales del usuario, como nombre, apellidos, entre otros.***

c) ***Los usuarios tienen las siguientes obligaciones:***
   - ***i. Deben cambiar la contraseña cada noventa (90) días, cumpliendo la condición de fortaleza señalado en el literal b) de este numeral.***
   - ***ii. No deben registrar la contraseña en documentos físicos, archivos o guardarlas en exploradores de internet (Google, Chrome, Edge).***
   - ***iii. Mantener absoluta confidencialidad de la contraseña, ya que es personal e intransferible.***
   - ***iv. Cambiar inmediatamente la contraseña ante cualquier sospecha de robo, compromiso o conocimiento por parte de terceros, y comunicar el incidente de seguridad a través del Sistema de Mesa de Servicios.***
   - ***v. Identificarse en el Sistema de Mesa de Servicios cuando se requiera el restablecimiento de la contraseña, utilizando las preguntas de seguridad previamente configuradas.***

7.1.16. ***Derechos de Acceso (A.5.18)***

Los derechos de acceso a los activos de información se brindan, teniendo en consideración lo siguiente:

a) ***Los propietarios de los activos de información establecen los derechos de acceso a sus activos y los revisan de forma trimestral.***

b) ***El personal de soporte técnico de la OTI atiende las solicitudes de*** acceso a los recursos informáticos como impresoras, carpetas de red y demás servicios informáticos***, a través del Sistema de Mesa de Servicios.***

c) ***Los responsables de las unidades de organización de la Sunass solicitan los accesos a los sistemas de información y a la "unidad de red H" para su personal, a través del Sistema de Mesa de Servicios, empleando la*** "GTI-OTI-FM003 Solicitud de Accesos y Privilegios a los Sistemas de Información de la Sunass", debidamente llenado ***y firmado.***

d) Cada seis (6) meses, el Especialista en Seguridad Informática de la OTI, revisa ***el estado de las cuentas*** de acceso de los usuarios***, contrastándolo con la lista de personal proporcionada por la URH y por los responsables de las unidades de organización, con la finalidad de identificar cuentas pendientes de baja u otras observaciones. Estas serán comunicadas al/ a la OSCD y al responsable de la unidad de organización que corresponda.***

7.1.17. ***Seguridad de la Información en las Relaciones con los Proveedores (A.5.19)***

a) ***Todo*** proveedor que presta servicios a la entidad y que tenga acceso a los activos de información y/o instalaciones de procesamiento de información, ***debe de conocer y cumplir la presente directiva***. ***Para tal fin,*** debe presentar dentro de la documentación para el inicio de la prestación de su servicio el formato de "GAF-CBS-FM005 Declaración jurada de compromiso de confidencialidad" debidamente firmado.

b) ***En caso la prestación del servicio/bien requiera la participación de personal del proveedor, ellos también deben cumplir con los lineamientos establecidos en la presente directiva. Es responsabilidad del proveedor implementar los controles necesarios para asegurar dicho cumplimiento y contar con las evidencias que lo sustenten***. En caso de incumplimiento, la Sunass se reserva el derecho de solicitar el cambio del personal, sin perjuicio del derecho de resolver el contrato de prestación de servicios/bien**.**

c) ***Todo proveedor debe acceder únicamente a los activos de información a los cuales se le haya otorgado autorización en el marco de la prestación del bien o servicio contratado, haciendo un uso y manejo adecuado de estos, protegiéndolos de accesos, modificaciones o eliminaciones no autorizadas***. ***Los proveedores deben dar cumplimiento a lo establecido en la sección "Respecto al uso aceptable de la información y de los activos asociados" de la presente directiva.***

7.1.18. ***Abordar la Seguridad de la Información dentro de los Acuerdos con Proveedores (A.5.20)***

a) ***Todo proveedor que tenga acceso a las instalaciones de la Sunass debe cumplir con lo establecido en la sección "Trabajo en Áreas Seguras" de la presente directiva. Así mismo, debe dar cumplimiento a las demás disposiciones de la presente directiva que correspondan según la naturaleza del bien o servicio contratado, así como de los activos involucrados, con el fin de garantizar la seguridad de la información por parte de estos.***

b) ***Toda información compartida o transferida al proveedor o que este haya conocido durante la prestación del servicio/bien contratado tendrá carácter confidencial, no debiendo ser utilizada, en ningún caso, para fines diferentes a los asociados al contrato, condición que se mantiene vigente incluso después de finalizado el contrato.***

c) ***El responsable de la unidad de organización en la que el proveedor preste el servicio/bien, debe evaluar la necesidad de que dicho proveedor participe en una charla de concientización sobre seguridad de la información, y de corresponder, debe comunicarlo al/ a la OSCD para la ejecución de esta.***

d) ***Todo proveedor debe notificar inmediatamente cualquier evento o incidente de seguridad o violación de datos que involucre información de la Sunass, a través del responsable del área usuaria donde se esté prestando el servicio/bien. Este, a su vez, debe comunicarlo al/ a la OSCD mediante los mecanismos internos establecidos.***

7.1.19. ***Gestión de la Seguridad de la Información en la cadena de suministro de las TIC (A.5.21)***
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.

7.1.20. ***Seguimiento, Revisión y Gestión de Cambios en Servicios de Proveedores (A.5.22)***

La Sunass cuenta con la potestad de realizar revisiones o auditorías (con personal interno o externo) para verificar que el proveedor cumple con las disposiciones de la presente directiva. En estos casos, el OSCD debe gestionar la revisión o auditoría.

7.1.21. ***Seguridad de la Información para el Uso de Servicios en la Nube (A.5.23)***

a) ***La OTI establece los requisitos para la contratación de los servicios en la nube y las responsabilidades del proveedor, garantizando el cumplimiento de los controles de seguridad y la normativa establecida por la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.***

b) ***Los proveedores de servicio en la nube son responsables, como mínimo, de lo siguiente:***

- ***i. Implementar mecanismos de autenticación, como el uso del múltiple factor de autenticación (MFA) u otras alternativas robustas de seguridad para asegurar que solo usuarios autorizados accedan a los recursos en la nube.***
- ***ii. Utilizar algoritmos de cifrado fuertes, como el cifrado avanzado AES (Advanced Encryption Standard) o superiores, para garantizar la seguridad de los datos almacenados y transmitidos.***
- ***iii. Implementar técnicas de borrado seguro de información, garantizando la eliminación completa y segura de los datos de sus sistemas en la nube al finalizar el contrato de servicio o en caso de una solicitud específica de la Sunass.***
- ***iv. Implementar políticas de respaldo y recuperación robustas considerando las especificaciones o requisitos técnicos establecidos por la OTI en los términos de referencia del servicio con la finalidad de garantizar la disponibilidad e integridad de la información. Estas políticas deben contemplar el uso de cifrado para proteger la información confidencial durante el proceso de respaldo.***
- ***v. Cumplir las leyes y regulaciones vigentes en materia de privacidad y seguridad de la información. Esto incluye, entre otros, el cumplimiento de regulaciones como la Ley de Protección de Datos Personales.***
- ***vi. Contar con procedimientos de monitoreo continuo para detectar de manera oportuna actividades sospechosas o no autorizadas, así como para la gestión de incidentes y vulnerabilidades.***

c) ***El personal o proveedor que requiera el uso de servicios en la nube para el cumplimiento de sus funciones o actividades debe solicitar la autorización del responsable de la unidad de organización a la que pertenece o brinda el servicio o bien para el que fue contratado. Esta autorización debe basarse en los servicios en la nube autorizados por la OTI, principalmente mediante el uso de la plataforma institucional Microsoft 365.***

7.1.22. ***Gestión de Incidentes de Seguridad de la Información (A.5.24, A.5.25, A.5.26, A.5.27 y A.5.28)***

a) ***Todo usuario debe comunicar cualquier situación de peligro, evento, incidente o debilidad de seguridad que involucre a los activos de información de la Sunass. El personal debe realizar esta comunicación a través del Sistema de Mesa de Servicios, y en el caso de personas externas, deben realizar la comunicación por medio del personal de contacto designado.***

b) La gestión de incidentes se realiza según lo establecido en la caracterización del proceso "GTI-AED-CR-N2 Atención de Eventos, Incidentes y Debilidades de Seguridad de la Información" y en el instructivo " GTI-OTI-IN001 Atención de eventos y debilidades de seguridad de la información", así como, de otras disposiciones que establezca la OTI para tal fin

7.1.23. ***Seguridad de la Información en Situaciones Disruptivas (A.5.29)***

a) ***Los usuarios deben de mantener la confidencialidad de sus contraseñas, las cuales son de uso personal e intransferible, protegiendo así su identidad digital.***

b) ***La OTI mantiene activo los controles de acceso a la infraestructura, aplicaciones, sistemas y servicios informáticos, así como los logs de auditoría y trazabilidad.***
c) ***La OTI debe garantizar que, en los ambientes de contingencia implementados para las aplicaciones o sistemas informáticos, se mantengan controles que protejan la confidencialidad, integridad y disponibilidad de la información, así como los niveles de acceso basado en perfiles autorizados.***
d) ***La OTI asegura la ejecución de las copias de respaldo, cuyo acceso está restringido sólo al personal autorizado.***
e) ***La OTI verifica que el traslado de las copias de respaldo para su restauración se realice de forma segura, protegiendo su confidencialidad, integridad y disponibilidad.***
f) ***En caso de traslados de información física, la UGD verifica que estos se realicen de forma segura, protegiendo su confidencialidad, integridad y disponibilidad.***
g) ***En caso de requerirse reemplazo del equipamiento informático, este debe de mantener la configuración base establecida por la OTI.***

7.1.24. ***Preparación de las TIC para la Continuidad del Negocio (A.5.30)***

a) ***La OTI establece el GDI-GCP-IG001 Plan de Contingencia de Sistemas de Información de la Sunass, que describe las acciones a realizar ante escenarios disruptivos, en alineamiento con el Plan de Continuidad Operativa de la Sunass.***
b) ***La Sunass cuenta con un Equipo de Respuestas ante Incidentes de Seguridad Digital – (CSIRT, por su denominación en inglés Computer Security Incident Response Team), el cual fue conformado mediante resolución de Presidencia Ejecutiva.***

7.1.25. ***Requisitos Legales, regulatorios y contractuales (A.5.31)***

a) La OAJ remite al/***a la OSCD*** 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".
b) El/ La ***OSCD*** debe coordinar con ***el o los responsables de las unidades de organización involucradas en la nueva norma legal identificada,*** con la finalidad de dar cumplimiento ***a las disposiciones emitidas.***

7.1.26. ***Derechos de Propiedad Intelectual (A.5.32)***

a) ***Todos los productos, creaciones, desarrollos, campañas, trabajos, investigaciones, u otros entregables, realizados por el personal o proveedores en cumplimiento de sus labores o actividades durante la vigencia de su contrato, son de propiedad de la Sunass.***
b) ***Toda la información registrada, mostrada, contenida y albergada en los equipos informáticos o dispositivos de punto final de usuario, aplicaciones, sistemas y servicios de la Sunass son de propiedad de la entidad.***
c) ***Los usuarios que hacen uso de equipos de cómputo de la Sunass no deben instalar o ejecutar programas o software no autorizados ni validados por la OTI. Asimismo, no deben copiar o compartir software, programas u otros contenidos que violen los derechos de autor.***
d) ***La OTI es responsable de implementar controles informáticos que eviten la instalación de software no autorizado o ilegal, así como de monitorear su cumplimiento.***

7.1.27. ***Protección de Registros (A.5.33)***
La OTI cumple con el resguardo ***y protección*** de los registros ***digitales a través*** de *backups* según lo establecido en la caracterización del proceso "GTI-RRI-CR-N2 Respaldo y restauración de la

información", ***y cuenta con controles de acceso para garantizar*** la confidencialidad, integridad y disponibilidad de la información ***digital*** que se emplea para la operatividad de los procesos de la Sunass.

7.1.28. ***Privacidad y Protección de la Información de Identificación de Personal – IIP (A.5.34)***
Todo personal o proveedor de la Sunass, debe dar cumplimiento a lo establecido en la Ley N° 29733 - Ley de Protección de Datos Personales, su reglamento, directivas y demás normas modificatorias, complementarias y conexas. El tratamiento de los datos personales debe realizarse única y exclusivamente para los fines establecidos, garantizando su confidencialidad, integridad y disponibilidad. La Sunass cuenta con un Oficial de Datos Personales, que es responsable de velar por el cumplimiento de las normas en materia de protección de datos personales en la entidad.

7.1.29. ***Revisión Independiente de la Seguridad de la Información (A.5.35)***
El/la Coordinador/a General del SIG debe revisar la programación de las auditorías del SGSI en coordinación con el/la ***OSCD*** 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.

7.1.30. ***Cumplimiento con Políticas, Reglas y Normas de Seguridad de la Información (A.5.36)***
Los responsables de las unidades 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 con lo establecido en la caracterización del proceso "GDI-NCA-CR-N3 Observaciones, No Conformidades y Acciones Correctivas para la Mejora del Sistema Integrado de Gestión".

7.1.31. ***Procedimientos Operativos Documentados (A.5.37)***
La Sunass controla la documentación de sus procedimientos operativos en el "Listado Maestro de Documentos", que se encuentra disponible en su portal del SIG (intranet).

7.2. CONTROLES DE PERSONAL

7.2.1. Selección (A.6.1)

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 "GRH-SDP-CR-N2 Selección del personal".

7.2.2. Términos y Condiciones del Empleo (A.6.2)

a) Las ***funciones,*** responsabilidades ***y obligaciones*** del personal, se encuentran definidos en los contratos.
b) El/la Jefe/a de la URH, solicita el alta de personal nuevo a la OTI mediante el Sistema de Mesa de Servicio, según lo establecido en la caracterización del proceso "GTI-ACI-CR-N3 Administración de cuentas institucionales".

7.2.3. ***Toma de Conciencia, Educación y Capacitación sobre Seguridad de la Información (A.6.3)***

a) 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.
b) 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.
c) 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 "GRH-IND-CR-N2 Inducción", con la participación del ***OSCD***.
d) 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 ***OSCD.***
e) Todo el personal de la Sunass debe asistir a las charlas, talleres o capacitaciones en Seguridad de la Información.

7.2.4. ***Respecto al Proceso Disciplinario (A.6.4)***

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

7.2.5. ***Respecto a las Responsabilidades Después del Cese o Cambio de Empleo (A.6.5)***

a) ***El personal, antes de su desvinculación, debe realizar la entrega de cargo, incluyendo la información contenida en la cuenta de correo electrónico institucional[1].***
b) 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.
c) Los derechos de acceso a la información y a las instalaciones de procesamiento del personal, es removido o modificado al producirse el término de la relación laboral o del contrato.
d) El/la Jefe/a de la URH solicita la baja del personal cesado a la OTI, según lo establecido en la caracterización del proceso "GTI-ACI-CR-N3 Administración de cuentas institucionales".

7.2.6. ***Acuerdos de Confidencialidad o no Divulgación (A.6.6)***

a) 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.
b) ***En los casos en que se requiera la habilitación de una cuenta desactivada que se encuentre en proceso de eliminación, se deberá contar con la autorización del titular de la cuenta, así como la del responsable de la unidad de organización a la que pertenecía.***

7.2.7. ***Respecto al Teletrabajo (A.6.7)***

a) 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.

[1] Artículo 37.2 del Reglamento de la Ley de Transparencia y Acceso a la Información Pública aprobada con el Decreto Supremo N° 007-2024-JUS

b) ***El personal que realiza teletrabajo debe cumplir con todas las disposiciones establecidas en la presente directiva y adicionalmente:***

i. ***Conectarse a las aplicaciones, sistemas y servicios informáticos de la Sunass desde ambientes físicos seguros que garanticen la privacidad de su trabajo y desde conexiones a internet confiables (no públicos, ni gratuitos) y que usen contraseñas de conexión seguras.***

ii. ***Realizar el bloqueo del equipo informático desde el que se conecta a las aplicaciones, sistemas y servicios informáticos de la Sunass, cuando se retire por algún motivo de su lugar de trabajo.***

iii. Brindar acceso al personal autorizado del ***Sistema de Mesa de Servicio*** 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.

iv. Verificar que el equipo informático asignado cuente con bloqueo automático por inactividad.

v. ***Asegurar*** 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.

vi. 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.

vii. 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.

c) ***La OTI debe:***

i. Asegurar que los equipos que se entreguen ***al personal*** cuenten con antivirus y Sistema Operativo actualizado, ***así como software VPN y software de administración remota autorizado instalados y configurados.***

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

iii. 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.

iv. Verificar que se ***cierren*** los accesos a los sistemas de información, cuando finalicen las actividades remotas.

7.2.8. Reporte de Eventos de Seguridad de la Información (A.6.8)

a) ***Todo usuario que tenga contacto con activos de información de la Sunass*** debe comunicar los eventos***, debilidades e incidentes de seguridad*** identificados ***a través del Sistema de Mesa de Servicios de la OTI;*** a fin de que se realicen las acciones necesarias.

b) El personal ***del Sistema de Mesa de Servicios sigue lo indicado en*** el instructivo “GTI-OTI-IN001 Atención de eventos y debilidades de seguridad de la información”.

7.3. CONTROLES FÍSICOS

7.3.1. Perímetros de Seguridad Física (A.7.1)

a) ***LA OAF es responsable de normar e implementar los controles para asegurar la seguridad física de las instalaciones de la Sunass, reforzando los controles para aquellos ambientes donde se almacena, procesa y/o resguarda información física o digital.***

b) ***El acceso al centro de datos es administrado por la OTI quien lleva el registro de visitas, este ambiente es físicamente sólido; los muros, paredes y pisos externos son sólidos y todas las puertas exteriores están protegidas contra accesos no autorizados mediante mecanismos de control biométrico.***

c) ***El acceso a los cuartos de comunicaciones es administrado por OTI y se brinda previa autorización.***

d) ***El acceso al Archivo Central es administrado por la UGD quien lleva el registro de las visitas, este ambiente es físicamente sólido; los muros, paredes y pisos externos son sólidos y todas las puertas exteriores están protegidas contra accesos no autorizados mediante mecanismos de control***.

7.3.2. ***Ingreso Físico (A.7.2)***

Se cuenta con personal de vigilancia, que verifica la autorización de ingreso a las instalaciones, registra el acceso ***y restringe al personal no autorizado.***

7.3.3. ***Asegurar Oficinas, Salas e Instalaciones (A.7.3)***

La UA asegura las oficinas, salas y demás ambientes de la Sunass a través del servicio de vigilancia y cámaras de video vigilancia.

7.3.4. ***Supervisión de la Seguridad Física (A.7.4)***

a) ***La OTI monitorea el acceso al centro de datos para detectar actividades sospechosas y supervisa los trabajos que se realicen en este.***

b) ***La UA, es responsable de supervisar el servicio de vigilancia y las cámaras de video vigilancia.***

7.3.5. ***Protección contra Amenazas Físicas y Ambientales (A.7.5)***

Las instalaciones de la Sunass cuentan con extintores operativos y cargados, alarmas contra incendios, rutas de evacuación y zonas seguras señalizadas.

7.3.6. ***Trabajo en Áreas Seguras (A.7.6)***

a) ***Cuando un tercero ingrese al centro de datos debe ser acompañado por un personal técnico autorizado de la OTI.***

b) ***Se encuentra prohibido tomar fotografías o filmar dentro de los ambientes donde se almacene o procese información confidencial, salvo se realice como parte de alguna acción legal y previa autorización del responsable de la unidad de organización que administra el ambiente.***

c) 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). (***Asociado también al control A.7.11)***

d) El personal autorizado (personal, y terceros) no debe facilitar el acceso a las instalaciones a personas desconocidas.

7.3.7. ***Escritorio y Pantallas Limpias (A.7.7)***

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:

a) 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 ***05 minutos***.
b) 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.
c) 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.
d) Cuando se imprima información confidencial, debe retirarse de forma inmediata de las impresoras.
e) La pantalla de autenticación a la red debe requerir solamente la identificación de la cuenta y una contraseña.
f) 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.

7.3.8. ***Ubicación y Protección de los Equipos (A.7.8)***

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, ***considerando lo siguiente:***

a) Deben de localizarse ***preferiblemente*** en ubicaciones que no queden expuestas al acceso de personas externas, ***en casos de ubicación*** en zonas de atención deben situarse de forma que las pantallas no puedan ser visualizados por personas externas.
b) 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.
c) El personal debe respetar y no modificar por ningún motivo la configuración de hardware y software establecida por la OTI.
d) El personal está prohibido de abrir los equipos de cómputo o dispositivos informáticos, excepto el personal especializado de la OTI.
e) 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.

7.3.9. ***Seguridad de los Activos Fuera de las Instalaciones (A.7.9)***

a) 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.
b) El uso de equipos ***informáticos*** de propiedad de la Sunass fuera de sus instalaciones debe ser autorizado de manera expresa por los ***responsables*** de cada unidad de organización. El personal autorizado asume la responsabilidad de la custodia del equipo***, por tanto, debe evitar dejarlo sin vigilancia y exponerlo a ambientes con condiciones extremas (temperatura, humedad, polvo).***

7.3.10. ***Medios de Almacenamiento (A.7.10)***

a) ***La OTI configura controles técnicos para bloquear los puertos USB de los equipos de cómputo y laptops, restringiendo la conexión de dispositivos de almacenamiento de información.***

b) ***El personal no debe guardar información de la Sunass en dispositivos de almacenamiento externos tales como memorias USB, pendrives, discos duros externos, celulares, entre otros).***

c) ***Para los casos de transporte o transferencia autorizada de medios de almacenamiento que contengan*** información confidencial, ***estos deben de considerar*** técnicas de cifrado, ***enmascaramiento*** o empaquetado (ZIP o RAR) y con clave para proteger los datos.

d) Los medios de almacenamiento ***que hayan sido autorizados tendrán un responsable asignado que deberá custodiarlo*** en un entorno seguro según las especificaciones del fabricante.

e) 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.

f) ***El responsable de medio de almacenamiento, cuando ya no requiere el uso de este, debe devolverlo a la OTI para ser reasignado o para su baja, donde se le realizará un proceso de borrado seguro.***

7.3.11. ***Seguridad del Cableado (A.7.12)***

El cableado de energía o de telecomunicaciones ***es*** protegido de cualquier intercepción o daño, para ello se ha establecido ***lo siguiente***:

a) 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.

b) ***La OTI es responsable de*** 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).

7.3.12. ***Respecto al Mantenimiento de Equipos (A.7.13)***

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

7.3.13. ***Respecto a la Eliminación Segura o Reutilización de Equipos (A.7.14)***

La OTI ***es responsable de realizar*** el borrado seguro ***de los equipos informáticos que contienen*** medios de almacenamiento, ***para su posterior*** entrega a la UA para la disposición de estos. El borrado seguro también se aplica en el caso que el ***equipo informático*** sea reutilizado por otro personal.

7.4. CONTROLES TECNOLÓGICOS

7.4.1. ***Dispositivos Terminales del Usuario (A.8.1)***

Los dispositivos de punto final de usuario deben de ser configurados y usados cumpliendo las siguientes disposiciones:

a) La UA realiza la asignación de dispositivos de punto final de usuario del tipo computadora de escritorio, smartphone, laptops, iPad y Tablets, y mantiene su inventario.

b) ***El personal debe proteger el dispositivo asignado y usarlo únicamente para el cumplimiento de sus funciones u obligaciones con la Sunass, evitando verse involucrado en acciones ilegales*** contrarias a la moral y las buenas costumbres o para fines ajenos a las ***establecidas por la entidad***. El ***personal*** es responsable de toda actividad realizada en el ***dispositivo de punto final de usuario***.

c) ***Todo personal que cuente con un dispositivo asignado debe asegurarse que éste cuenta*** con mecanismos de autenticación como clave, patrón[2], ***PIN,*** huella digital, etc.

d) Todo ***personal que cuente con un dispositivo del tipo Tablet, Ipad, smartphone de propiedad de la Sunass es responsable de mantenerlo actualizado, asegurando que cuente*** con la última versión o la versión más segura de los sistemas operativos**,** los parches y aplicaciones provenientes del fabricante.

e) ***El personal solo debe guardar la información*** en la ubicación: "Mis documentos", la unidad H o el OneDrive.

f) Todo personal con acceso a un dispositivo de punto final de usuarios debe bloquear el dispositivo asignado, cuando se retira de su estación de trabajo o deja de hacer uso de este.

g) La OTI debe configurar el perfil del usuario, los accesos, correo electrónico y antivirus en el equipo de cómputo o laptop asignado.

h) La OTI es responsable de la configuración y actualización de los programas y sistema operativo de los equipos de cómputo y laptops. En el caso de laptops adicionalmente se cifra el dispositivo de almacenamiento interno.

i) La OTI debe configurar los dispositivos para que el usuario no pueda deshabilitar o modificar la funcionalidad de seguridad, así como instalar o desinstalar aplicaciones.

j) El personal no debe de configurar su correo electrónico personal (Hotmail, Google, etc.), redes sociales o servicios externos personales en dispositivos institucionales.

k) El personal no debe utilizar licencias personales en dispositivos institucionales.

l) ***El personal que cuenten con un dispositivo de usuario final*** debe evitar dejarlo en cajones sin seguro, lugares de reunión, autos o ambientes sin supervisión; manteniéndolo en lugares que ofrezcan seguridad.

m) La OTI realiza el borrado seguro para los dispositivos de usuario final antes de la reasignación o baja.

n) El personal no debe de formatear los dispositivos de punto final de usuario asignados., salvo el personal de la OTI que esté autorizado.

o) El personal no debe de guardar información confidencial en los dispositivos del tipo smartphone, Tablet, Ipad y evitar la conexión a redes Wi-Fi abiertas o que no sean de confianza.

p) El personal no debe entregar o prestar a otra persona los dispositivos del tipo laptop, smartphone, Tablet, Ipad. Además, debe ser prudente al responder mensajes o llamadas especialmente de números o remitentes desconocidos.

q) En caso de pérdida o robo, el personal en un máximo de 24 horas debe realizar la denuncia policial respectiva y debe comunicar inmediatamente a/ a la Jefe/a de la UA y a través del ***Sistema de Mesa de Servicios*** de la OTI, a fin de que se realicen las acciones correspondientes. ***Adicionalmente, ante la pérdida o robo*** 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.

7.4.2. ***Derechos de Acceso Privilegiados*** **(A.8.2)**

a) La cuenta de administrador ***es una cuenta privilegiada*** que sólo debe ***utilizarse*** para realizar actividades administrativas y no para navegación por internet, correo electrónico o actividades similares, ***por tanto,*** los administradores de los sistemas operativos***, servidores*** y base de datos deben tener cuentas segregadas ***para diferenciar sus actividades de administración a las de usuario común***.

b) El/la Jefe/a de la OTI designa los roles de administrador mediante la emisión de un memorando.

[2] El patrón y PIN solo serán usados para los Smartphone, Tablet.

c) El inventario de contraseña de los super usuarios será almacenada por sobre lacrado y estará bajo custodia ***del/ de la Jefe/a de la OTI.***
d) 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.
e) Ningún usuario/a debe contar con privilegio de administrador, en caso sea requerido ***por el responsable de la unidad de organización***, este/a debe solicitarlo por el ***Sistema de Mesa de Servicios*** 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/la ***OSCD.***
f) Los sistemas informáticos de la Sunass deben utilizar cuentas ***sólo con privilegios estrictamente necesarios*** para su operación o funcionamiento.
g) ***Ningún usuario/a debe*** poseer, desarrollar o ejecutar programas que pudieran dañar o alterar los recursos informáticos de la entidad.
h) ***En el caso que los responsables de las unidades de organización soliciten acceso a las bases de datos para la obtención de reportes u otras acciones, esta solicitud debe ser revisada previamente por el/la OSCD, quien evalúa el riesgo asociado a la información y/o base de datos.***

7.4.3. *Restricciones de Acceso a la Información (A.8.3)*

a) ***La OTI controla el acceso a la información digital, los sistemas, infraestructura y servicios informáticos a través de la identificación y autenticación del usuario (por ejemplo, usuario y contraseña),*** a fin de evitar accesos no autorizados, así mismo, los derechos de acceso ya sea de lectura, modificación, ***eliminación y ejecución son*** controlados.
b) 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.

7.4.4. *Acceso al Código Fuente (A.8.4)*

La OTI es responsable de controlar el acceso al código fuente de los programas, ***estableciendo que*** sólo es accesible por los desarrolladores a su proyecto asignado, desde la plataforma de desarrollo colaborativo de software.

7.4.5. *Autenticación Segura (A.8.5)*

La OTI establece como método de autenticación principal las credenciales de red, adicionalmente para los servicios soportados en Microsoft 365 usará el doble factor de autenticación. Existiendo sistemas legados donde no se puede integrar a una solución de autenticación única, asegurará que el medio usado para este fin sea seguro.

7.4.6. *Gestión de Capacidad (A.8.6)*

La OTI es responsable de gestionar la capacidad de las tecnologías de la información, supervisando el uso de los recursos y se hacen proyecciones de los futuros requisitos de capacidad tecnológica para asegurar el desempeño requerido de los sistemas de información.

7.4.7. *Protección contra Programas Maliciosos (A.8.7)*

Con la finalidad de reducir la presencia de software maliciosos en los sistemas de información y los medios de procesamiento, se establece lo siguiente:

a) El sistema de protección de códigos maliciosos debe encontrarse habilitado y actualizado en los equipos de la entidad; así como, en los equipos de personal de terceros o visitas que requieran ingresar a la red principal de la entidad.

b) La OTI es responsable de instalar, configurar, monitorear y controlar el sistema de protección de código malicioso en las estaciones de trabajo.
c) Todo incidente de infección de virus informático debe ser reportado inmediatamente ***a través del Sistema de Mesa de Servicios*** para su revisión ***y rápida atención***, a su vez, lo comunica al/ a la ***OSCD.***
d) El usuario no debe abrir archivos adjuntos a un correo electrónico que provengan de una fuente desconocida, sospechosa o no confiable.
e) Todos los usuarios deben reportar al ***Sistema de Mesa de Servicios*** de la OTI los correos spam, cadenas u otros correos electrónicos no deseados.
f) ***El usuario no debe*** 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.

*7.4.8. **Respecto a la Gestión de Vulnerabilidades Técnicas (A.8.8)***

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, ***los hallazgos y recomendaciones de esta revisión deben ser analizadas e implementadas, de ser el caso***.
b) El ***equipo*** de infraestructura tecnológica de la OTI ***realiza las gestiones a fin de*** 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 al/ a la Jefe/a de la OTI sobre el estado de la red informática de la entidad.
c) 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.
d) Los/a usuarios/as no cuentan con acceso para instalar aplicativos en sus equipos, el personal del ***Sistema de Mesa de Servicios*** de la OTI debe realizar la instalación de los aplicativos, previa autorización ***del responsable*** de la unidad de organización que corresponda.
e) El/La ***OSCD*** 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.

*7.4.9. **Respecto a la Gestión de la Configuración (A.8.9)***

Las configuraciones de los sistemas, de las redes, de los equipos de seguridad y del hardware son documentadas por la OTI y se mantienen protegidas. Esta documentación es esencial para la recuperación ante cualquier incidente y se pueda revisar las configuraciones iniciales o previas a cualquier cambio. Todos los cambios en las configuraciones deben estar registradas y almacenadas de forma segura.

*7.4.10. **Respecto a la Eliminación de Información (A.8.10)***

a) La información almacenada en cualquier medio (sistemas, dispositivos, etc.) que haya sido autorizada para su eliminación por el responsable de la unidad de organización, de acuerdo con las regulaciones vigentes, debe ser eliminada utilizando métodos que aseguren que este proceso sea seguro.
b) 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 OSCD.

c) Los documentos confidenciales en papel considerados como desecho deben ***destruirse o*** triturarse antes de retirarlos de las instalaciones de la Sunass.

7.4.11. ***Respecto al Enmascaramiento de Información (A.8.11)***

a) Para la protección de la información que se gestiona, especialmente la relacionada a datos personales, de ser posible, esta debe estar enmascarada para limitar su exposición. Para tal fin, se puede utilizar técnicas de seudonimización o anonimización. Cada unidad de organización debe identificar y determinar la información que requiere ser enmascarada e informarlo al/ a la OSCD.

b) El/La Coordinador/a de Desarrollo Tecnológico de la OTI debe determinar, en base a las mejores prácticas, el método de enmascaramiento de información más adecuado para cada caso.

7.4.12. ***Respecto a la Prevención de Fuga de Datos (A.8.12)***

a) Los equipos de cómputo y laptops cuentan con los puertos USB bloqueados, con el fin de prevenir la extracción no autorizada de información sensible.

b) La OTI implementa restricciones de navegación para prevenir la fuga de información.

7.4.13. ***Respecto a la Copia de Seguridad de la Información (A.8.13)***
La OTI es responsable del respaldo de la información digital, software y sistemas de la Sunass, por lo cual se dispone:

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) ***La OTI lleva a cabo*** el respaldo y las pruebas de recuperación de la información según lo establecido en la caracterización del proceso "GTI-RRI-CR-N2 Respaldo y restauración de la información" y en el instructivo de "GTI-OTI-IN002 Ejecución del respaldo y restauración de la información".

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.

7.4.14. ***Respecto a la Redundancia de las Instalaciones de Procesamiento de Información (A.8.14)***
La OTI es responsable de implementar infraestructura tecnológica de procesamiento de información redundante con capacidad suficiente para garantizar la disponibilidad de los servicios de TI.

7.4.15. ***Respecto al Registro (A.8.15)***
La OTI es responsable de gestionar los registros (logs) generados por la infraestructura y los servicios informáticos de la entidad. Para tal fin, se establece lo siguiente:

a) 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.

b) 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.
c) Los registros de los servicios críticos (logs del sistema) deben ser consolidados y almacenados en una plataforma ***para*** ser conservados por un periodo de 6 meses.
d) ***Está prohibido*** intentar distorsionar o falsear los registros "logs" de los sistemas de información.

7.4.16. ***Respecto a las Actividades de Monitoreo (A.8.16).***
La OTI realiza un monitoreo constante a las redes y a los sistemas para detectar eventos inusuales y comunicar su ocurrencia a los roles responsables para la toma de acciones correspondientes. Para ello, se establece lo siguiente:

a) Se debe monitorear el tráfico de red, el acceso a los sistemas, servidores y equipos de red, así como los registros de eventos relacionados con la actividad del sistema y la red.
b) Se debe supervisar el uso y rendimiento de los recursos tecnológicos, tales como CPU, discos duros, memoria y ancho de banda.
c) La Sunass se reserva el derecho de activar ***el monitoreo*** sobre los mensajes enviados o recibidos para verificar el cumplimiento de los lineamientos establecidos para el uso del correo electrónico.

7.4.17. ***Respecto a la Sincronización del Reloj (A.8.17)***
La OTI debe asegurar que todos los equipos de la red se conectan al servidor de dominio para su sincronización de actualización de los relojes.

7.4.18. ***Respecto al Uso de Programas de Utilidad Privilegiados (A.8.18)***

a) El uso de programas utilitarios que vulneren los controles de seguridad no debe ser instalados ni utilizados bajo sanción como se estipula en el RIS.
b) 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.
c) ***El Sistema de Mesa de Servicios*** 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, ***para su evaluación***.

7.4.19. ***Respecto a la Instalación de Software en Sistemas Operativos (A.8.19)***
La OTI es responsable de gestionar el software en la entidad. Para ello, se establece lo siguiente:

a) Sólo se permite el uso de software aprobado por la OTI, siendo el personal autorizado para realizar la instalación el de soporte técnico.
b) Los usuarios ***no*** deben descargar, instalar, copiar, acceder, ejecutar o emplear ***software o programas ilegales, sin licencia, piratas o de su propiedad.***
c) ***El personal de soporte técnico*** 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.

7.4.20. ***Respecto a la Gestión de Seguridad de la Red (A.8.20, A.8.21 y A.8.22)***

Respecto al control A.8.20

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 al Sistema de Mesa de Servicios 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.
   En los equipos de los usuarios nuevos deberá mostrarse un banner al encender el equipo ***sobre la atención por el Sistema de Mesa de Servicios.***

Respecto al control A.8.21:

d) El ***personal*** 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/ a la *OSCD***.**
e) La seguridad en los servicios de las redes es administrada y gestionada por personal de infraestructura tecnológica de la OTI.
f) Los equipos de comunicaciones cumplen los requisitos mínimos de seguridad establecidos.

Respecto al control A.8.22:

g) En la red interna se tiene habilitado la red de WIFI y solo tienen acceso los usuarios de red.
h) 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.
i) El acceso inalámbrico está protegido mediante contraseñas complejas.
j) 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.
k) Asegurar que todo dispositivo que se conecte a la red de la Sunass cuente con antivirus y sistema operativo actualizado

7.4.21. ***Respecto al Filtrado Web (A.8.23)***

a) La OTI bloquea sitios web que no son requeridos para la ejecución de las actividades de la Sunass.
b) En el caso que una unidad de organización requiera acceso a un sitio web no autorizado, debe de comunicarlo a la OTI para que se evalúen los impactos de malware o información ilegal antes de brindar el acceso
c) 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 ***OSCD***

7.4.22. ***Respecto al Uso de la Criptografía (A.8.24)***

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.

7.4.23. ***Respecto al Ciclo de Vida de Desarrollo Seguro (A.8.25)***

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

a) Los entornos de desarrollo, pruebas y producción deberán estar segregados.
b) Se debe asegurar el entorno de desarrollo considerando que los miembros del equipo de desarrollo son los únicos que tienen acceso autorizado al mismo.
c) Las aplicaciones deben ser desarrolladas utilizando lenguajes y técnicas de programación segura, tomando en cuenta los lineamientos específicos de control de accesos.
d) En el desarrollo de aplicaciones WEB, se debe utilizar el estándar de verificación de seguridad de aplicaciones OWASP (top 10).
e) 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.
f) 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.
g) Se debe evitar el acceso no autorizado a las fuentes del software, debiendo el acceso a dichos repositorios ser controlado.
h) 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.
i) Todas las aplicaciones web se deben ofrecer exclusivamente mediante HTTPS.
j) Los registros de eventos de aplicaciones web se almacenan de forma centralizada.
k) Para el desarrollo de aplicaciones se utilizan las prácticas de DevOps.

7.4.24. ***Respecto a los Requisitos de Seguridad de las Aplicaciones (A.8.26)***

a) Los presentes lineamientos deben adoptarse en el desarrollo, adquisición de nuevos sistemas de información o mejoras de los existentes.
b) La información involucrada en los servicios de aplicación que pasan a través de redes públicas debe ser protegida con la aplicación de mecanismos seguros como https, cifrado de información, uso de firmas digitales, entre otros
c) 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.
d) Se debe aplicar controles de seguridad basados en una “Evaluación de riesgos”.
e) Se deben revisar el cumplimiento de obligaciones/expectativas legales.
f) 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.
g) 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.
h) 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.
i) 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.

j) 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.
k) 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.
l) Verificar que toda autenticación exitosa y re-autenticaciones generen un nuevo identificador de sesión.
m) Verificar que los identificadores de sesión son suficientemente largos, aleatorios y únicos para las sesiones activas.
n) 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.
o) Verificar que datos almacenados del cliente no contengan información sensible o información personal identificable.

7.4.25. ***Respecto a la Arquitectura de Sistemas Seguros y Principios de Ingeniería (A.8.27):***

Los principios de ***arquitectura e*** ingeniería de sistemas seguros establecidos son:

a) Las aplicaciones cuentan con mecanismos de autenticación difíciles de vulnerar.
b) En los casos que se requiera, aplicar el uso correcto de la criptografía.
c) Partir de un mínimo modelo de permisos y luego ir escalando privilegios;
d) Limpiar la codificación de pruebas.
e) Aplicar validaciones para el registro de datos según corresponda.
f) Hacer seguimiento de las versiones y tecnologías usadas ya que estás van evolucionando o se vuelven obsoletas.
g) Las claves pasan por un proceso de encriptación.
h) Los cambios que se soliciten deben pasar por un proceso de evaluación y deben ser documentados.

7.4.26. ***Respecto a la Codificación Segura (A.8.28)***

La Sunass establece los lineamientos generales para que el software se escriba de forma segura, reduciendo así la cantidad de posibles vulnerabilidades de seguridad de la información, por lo que se considera lo siguiente:

a) Validación y sanitización de entradas: Asegurar la validación de todos los datos de entrada (como formularios, URL, parámetros) para evitar inyecciones (SQL, XSS, etc.).
b) Autenticación segura: Utilizar algoritmos robustos como bcrypt o Argon2 para almacenar contraseñas. En plataformas web, utilizar HTTPS para proteger las credenciales en tránsito. Implementación de un SSO, que almacene las contraseñas de forma segura y la implementación de autenticación multifactor (2FA)
c) Cifrado de Datos: Cifrado de los datos sensibles, tanto en tránsito (con SSL/TLS) como en reposo (en bases de datos y almacenamiento).
d) Control adecuado de privilegios: Asegurar de que los usuarios y servicios solo tengan acceso a lo que necesitan, ni más ni menos. Definir roles y permisos claramente, para que los usuarios no tengan permisos excesivos.
e) Revisión y auditoria de código: Realizar revisiones regulares de código para detectar posibles vulnerabilidades a través del uso de herramientas automáticas de análisis de seguridad (como SonarQube, Checkmarx, etc.).

7.4.27. ***Respecto a las Pruebas de Seguridad en Desarrollo y Aceptación (A.8.29)***

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 ***GTI-ITI-FM003 Solicitud de Cambio o Nuevo Requerimiento de Sistema Informático***.

7.4.28. ***Respecto al Desarrollo Subcontratado (A.8.30)***

La OTI establece los requisitos de seguridad para desarrollo subcontratado en los términos de referencia del servicio en concordancia con las secciones "***Ciclo de Vida de Desarrollo Seguro", "Requisitos de Seguridad de las Aplicaciones", "Arquitectura de Sistemas Seguros y Principios de Ingeniería"," Codificación Segura", "Pruebas de Seguridad en Desarrollo y Aceptación" de la presente Directiva.*** *Así mismo*, supervisa su cumplimiento.

7.4.29. ***Respecto a la Separación de los Entornos de Desarrollo, Prueba y Producción (A.8.31)***

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

7.4.30. ***Respecto a la Gestión de los Cambios (A.8.32)***

a) Para la revisión técnica de aplicaciones después de cambios en la plataforma operativa:
   i. 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.
   ii. 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.
   iii. 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.

b) 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.

c) Todo cambio en los 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:

   i. 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.

ii. 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.

iii. 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.

iv. 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 al/ a la Jefe/a de la OTI con copia al ***OSCD***, 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.

7.4.31. ***Respecto a los Datos de Prueba (A.8.33)***

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.

7.4.32. ***Respecto a los Controles de Auditoría de Sistemas de Información (A.8.34)***

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.