SUPERINTENDENCIA NACIONAL DE BIENES ESTATALES

RESOLUCIÓN Nº 0016-2021/SBN

San Isidro, 19 de febrero de 2021

VISTOS:

El Acta de Reunión N° 16-2021-CGD de fecha 18 de febrero de 2021, del Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales; el Informe N° 00003-2021/SBN-CGD de fecha 19 de febrero de 2021, del Secretario Técnico del Comité de Gobierno Digital; el Informe N° 00155-2021/SBN-OPP de fecha 19 de febrero de 2021, de la Oficina de Planeamiento y Presupuesto; el Informe N° 00041-2021/SBN-OAJ de fecha 19 de febrero de 2021, de la Oficina de Asesoría Jurídica; y,

CONSIDERANDO:

Que, mediante la Resolución Ministerial N° 004-2016-PCM, modificada por la Resolución Ministerial N° 166-2017-PCM, se dispone el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad de la Información. Requisitos. 2º Edición", para todas las entidades integrantes del Sistema Nacional de Informática;

Que, en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad de la Información. Requisitos. 2º Edición", se dispone que la alta dirección debe establecer una política de seguridad de la información que es apropiada al propósito de la organización, incluye objetivos de seguridad de la información o proporciona el marco de referencia para fijar sus objetivos, un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información, un compromiso de mejora continua del sistema de gestión de seguridad de la información, y debe estar disponible como información documentada, estar comunicada dentro de la organización y disponible a las partes interesadas, según sea apropiado;

Que, con la Resolución N° 065-2018/SBN de fecha 7 de septiembre de 2018, modificada por las Resoluciones N°s 0074-2018/SBN y 0092-2018/SBN de fechas 27 de setiembre y 17 de diciembre de 2018, y por la Resolución N° 024-2019/SBN de fecha 1 de abril de 2019, se establece la conformación del Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales, el cual cuenta con las funciones de

promover y gestionar la implementación de estándares y buenas prácticas en seguridad digital, identidad digital y datos en la entidad, vigilar el cumplimiento de la normatividad relacionada con la implementación de la seguridad de la información y otras funciones que se le asigne en el ámbito de su competencia y aquellas concordantes con la materia;

Que, mediante el literal a) del numeral 6.3.2 de la Directiva N° 002-2017/SBN "Disposiciones para la Emisión de Documentos Normativos en la SBN", aprobada con la Resolución N° 051-2017/SBN de fecha 28 de junio de 2017, se dispone que cada órgano o unidad orgánica de acuerdo a las necesidades institucionales y según su competencia, podrá elaborar y proponer proyectos de documentos normativos ante las instancias respectivas para la opinión técnica favorable, adjuntando el informe que sustente su aprobación, también se expresa que la estructura de los documentos se desarrolla según corresponda, de acuerdo a lo indicado en el Anexo N° 1; asimismo, en el numeral 6.3.4 se indica que las políticas a nivel interno institucional son aprobadas por el Superintendente Nacional de Bienes Estatales, previa visación de la Oficina de Planeamiento y Presupuesto, de la Oficina de Asesoría Jurídica, la unidad de organización que la formula y las unidades de organización involucradas, de igual modo, señala que para su aprobación, el proyecto normativo debe contar con la opinión técnica favorable de la Oficina de Planeamiento y Presupuesto y de la Oficina de Asesoría Jurídica;

Que, en virtud a lo dispuesto en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 y la Directiva N° 002-2017/SBN, el Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales a través del Acta de Reunión N° 16-2021-CGD de fecha 18 de febrero de 2021, dio cuenta de la revisión del documento POL-001-2021/SBN-OAF-TI "Políticas de la Seguridad de la Información", brindó su conformidad al mismo y manifestó que se prosiga con el trámite de aprobación establecido en la Directiva N° 002-2017/SBN;

Que, en ese sentido, con el Informe N° 00003-2021/SBN-CGD de fecha 19 de febrero de 2021, el Secretario Técnico del Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales, sustenta técnicamente la propuesta POL-001-2021/SBN-OAF-TI "Políticas de la Seguridad de la Información" señalando que la seguridad de la información es la protección de toda información contra una amplia gama de amenazas con el fin de garantizar la continuidad de la institución y minimizar los riesgos informáticos en la Superintendencia, lo que permitirá conocer, tratar y minimizar los posibles riesgos que atenten contra la seguridad de la información en la SBN; por lo que recomienda la aprobación del documento propuesto;

Que, mediante el Informe N° 00155-2021/SBN-OPP de fecha 19 de febrero de 2021, la Oficina de Planeamiento y Presupuesto expresa que la unidad de organización proponente ha cumplido con emitir el informe sustentatorio, el mismo que contiene los fundamentos que justifican la elaboración y propuesta del documento normativo basado en el literal a) del numeral 6.3.2 de la Directiva N° 002- 2017/SBN y que el proyecto de Política se ajusta a lo señalado en el literal b) del numeral 6.3.2 Formulación de la Directiva N° 002-2017/SBN, que establece que la estructura de los documentos normativos se desarrollará de acuerdo a lo indicado en el Anexo N° 1, correspondiendo en el presente caso, el literal a) Estructura de una Política; por tales razones emite

opinión técnica favorable al proyecto POL-001-2021/SBN-OAF-TI “Políticas de la Seguridad de la Información”;

Que, a través del Informe N° 00041-2021/SBN-OAJ de fecha 19 de febrero de 2021, la Oficina de Asesoría Jurídica manifiesta que el proyecto POL-001-2021/SBN-OAF-TI “Políticas de la Seguridad de la Información”, propuesto y sustentado por el Secretario Técnico del Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales con el Informe N° 00003-2021/SBN-CGD, cumple con las disposiciones previstas en la Directiva N° 002-2017/SBN denominada “Disposiciones para la Emisión de Documentos Normativos en la SBN”, aprobada por la Resolución N° 051-2017/SBN; por lo que emite opinión legal favorable al proyecto normativo de alcance institucional;

Que, atendiendo a las consideraciones antes expuestas, resulta necesario aprobar el documento POL-001-2021/SBN-OAF-TI “Políticas de la Seguridad de la Información”, con la finalidad de asegurar la confidencialidad, integridad y disponibilidad de manera segura de la información de la Superintendencia Nacional de Bienes Estatales;

Con el visado de la Gerencia General, el Ámbito de Tecnologías de la Información, el Sistema Administrativo de Personal, la Unidad de Trámite Documentario, la Oficina de Asesoría Jurídica, la Oficina de Planeamiento y Presupuesto, el Líder del Gobierno Digital y el Oficial de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales;

De conformidad con lo dispuesto en la Resolución Ministerial N° 004-2016-PCM, la Resolución N° 065-2018/SBN, la Directiva N° 002-2017/SBN aprobada por la Resolución N° 051-2017/SBN; y, conforme a las funciones previstas en los literales r) y s) del artículo 11 del Reglamento de Organización y Funciones de la Superintendencia Nacional de Bienes Estatales, aprobado por el Decreto Supremo N° 016-2010-VIVIENDA;

SE RESUELVE:

Artículo 1.- Aprobar el documento POL-001-2021/SBN-OAF-TI “Políticas de la Seguridad de la Información”, que en Anexo forma parte integrante de la presente Resolución.

Artículo 2.- Disponer que la presente Resolución y su Anexo sea notificada a los integrantes del Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales – SBN, para los fines pertinentes.

Artículo 3.- Disponer que el documento POL-001-2021/SBN-OAF-TI “Políticas de la Seguridad de la Información”, aprobado en el artículo 1 de la presente resolución, es de cumplimiento obligatorio por los servidores civiles de la Superintendencia Nacional de Bienes Estatales.

Artículo 4.- Publicar la presente Resolución y su Anexo en el día de su emisión, en el Intranet de la SBN y en el Portal Institucional (www.sbn.gob.pe).

Regístrese y comuníquese.

Visado por:

Firmado digitalmente por: CAMPOS OBREGON Angel Benigno FAU 20131057823 hard
Fecha: 19/02/2021 17:25:36-0500

OAJ

Firmado digitalmente por: RONDON CHAVEZ Jorge Luis AUT 06157584 hard
Fecha: 19/02/2021 17:34:07-0500

TI

Firmado digitalmente por: LOAYZA CESPEDES Jorge Luis FAU 20131057823 hard
Fecha: 19/02/2021 18:16:00-0500

SAPE

Firmado digitalmente por: FLEMING VILLANO Frank FIR 42724993 hard
Fecha: 19/02/2021 18:17:20-0500

UTD

Firmado digitalmente por: LLAMOJA CABANILLAS Paul Alex FAU 20131057823 hard
Fecha: 19/02/2021 18:19:23-0500

OPP

Firmado digitalmente por: PALOMINO RAMIREZ Diana Sofia FAU 20131057823 hard
Fecha: 19/02/2021 18:23:00-0500

LGD

Firmado digitalmente por: BRAVO HERRERA Juan David FAU 20131057823 soft
Fecha: 19/02/2021 18:25:27-0500

OSI

Firmado digitalmente por: LOPEZ ENDO Jaime Eduardo FAU 20131057823 hard
Fecha: 19/02/2021 18:30:27-0500

GG

Firmado por:

Firmado digitalmente por: SUBAUSTE BRACESCO Armando Miguel FAU 20131057823 hard
Fecha: 19/02/2021 19:25:30-0500

Superintendente Nacional de Bienes Estatales

TIPO DE DOCUMENTO:

POLÍTICA

NOMBRE DEL DOCUMENTO:

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

NÚMERO DEL DOCUMENTO:

POL-001-2021/SBN-OAF-TI

NOMBRE DE LA UNIDAD DE ORGANIZACIÓN:

ÁMBITO DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA OFICINA DE ADMINISTRACIÓN Y FINANZAS

San Isidro, febrero de 2021

Versión N° 1.0

Contenido

POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

1. INTRODUCCIÓN

La seguridad de la información es la protección de toda información contra una amplia gama de amenazas con el fin de garantizar la continuidad de la institución y minimizar los riesgos informáticos en la SBN.

La gestión de la seguridad de la información es una herramienta que nos va a permitir conocer, tratar y minimizar los posibles riesgos que atenten contra la seguridad de la información en la SBN.

2. OBJETIVO

Asegurar la confidencialidad, integridad y disponibilidad de la información de la SBN.

3. MARCO JURÍDICO

3.1. Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de Seguridad de la Información, Requisitos. 2da. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, modificada por Resolución Ministerial N° 166-2017-PCM.

3.2. Resolución N° 038-2020/SBN del 12 de junio de 2020, que aprueba el Plan Estratégico Institucional de la SBN (PEI) 2020-2023 Modificado de la Superintendencia Nacional de Bienes Estatales.

3.3. Resolución Ministerial N° 340-2020-VIVIENDA, que aprueba la ampliación del Horizonte Temporal del Plan Estratégico Sectorial Multianual (PESEM) 2016-2021 del Sector Vivienda, Construcción y Saneamiento, al año 2024, denominándose "Plan Estratégico Sectorial Multianual (PESEM) 2016-2024 del Sector Vivienda, Construcción y Saneamiento".

3.4. Norma ISO/IEC 27001:2013, objetivos de control A.7.1, A.7.2, A.7.3, A.8.1.3, A.9.1, A.9.2, A.9.3, A.9.4, A.11.2.8, A.11.2.9, A.15.1 y A.15.2.

4. PRINCIPIOS

4.1. Disponibilidad: Característica de la Información por la cual se garantiza que se puede acceder a dicha información en cualquier momento.

4.2. Integridad: Característica de la Información que busca mantener con exactitud dicha información tal cual como fue generada, por la cual sólo es modificada por personas y/o sistemas autorizados y de una forma permitida.

4.3. Confidencialidad: Característica de la información por la cual se asegura que dicha información sea de conocimiento solamente para las personas y/o sistemas autorizados.

4.4. Protección: Acción y efecto de proteger o resguardar la información.

4.5. Acceso autorizado: Resultado de una autentificación correcta.

5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN

La SBN tiene como activo principal la información de los predios estatales registrados adecuadamente para su oportuna entrega a la ciudadanía de acuerdo al marco normativo vigente; dentro del cual, aplica mecanismos de protección para garantizar y asegurar la confidencialidad, disponibilidad e integridad de la información en cada uno de sus procesos frente a amenazas internas o externas, asumiendo el compromiso de proteger los recursos de información de la institución, así como de promover el desarrollo de una cultura de seguridad de la información y respaldar el apoyo constante durante la planificación, implementación, revisión y mejora continua del Sistema de Gestión de Seguridad de la Información.

6. ESTRATEGIA

La estrategia de implementación de la política de seguridad de la información en la SBN es una acción que requiere de la participación de toda la organización, incluyendo el respaldo y conducción de la alta dirección de la entidad, para ello, se debe asegurar la regulación normativa pertinente y que todos los/las servidores(as) civiles de la institución, así como del personal externo, conozcan, acepten y se familiaricen con la política establecida, la regulación emitida y con lo siguiente, según corresponda:

6.1. <u>Para la protección de la información móvil que pueda estar contenida en computadores portátiles, documentos en papel y en general cualquier tipo de información móvil que es utilizada en la SBN</u>

a) En computación Móvil

i. El dispositivo de computación móvil personal es propiedad de la SBN.

ii. Se tiene permitido el uso del dispositivo móvil personal de propiedad de los/las servidores(as) de la SBN, bajo regulación específica establecida en la normativa interna de la SBN.
iii. El personal es responsable por el cuidado general del dispositivo de computación móvil entregado por la SBN.

b) En el transporte de los dispositivos de computación móvil personal
La responsabilidad de cuidado recae sobre el/la usuario(a) que transporta el dispositivo de computación móvil.

c) En el acceso Remoto
i. La SBN valida las conexiones remotas para el uso de los/las servidores(as) civiles y los recursos internos.
ii. El Ámbito de Tecnologías de la Información (TI) registrará los permisos y accesos remotos a la red interna las veces que se realice dichas actividades y reportará las acciones al/a la CISO.

6.2. <u>Para una correcta gestión de los recursos humanos en la SBN</u>

a) En la verificación de antecedentes y contratación
i. El Sistema Administrativo de Personal (SAPE) es responsable de la verificación de los antecedentes laborales y de los grados y títulos de los/las nuevos(as) servidores(as).
ii. La contratación de nuevos(as) servidores(as) es canalizada a través del SAPE, según el procedimiento correspondiente.

b) Inducción
i. Los/las nuevos(as) servidores(as) de la SBN pasarán por un proceso de inducción a la política, estrategias, procedimientos y estándares de seguridad de la información, organizado por el SAPE.
ii. La inducción deberá ser planificada y realizada de forma mensual.
iii. El/la CISO o quién el Supervisor de Tecnologías de la Información determine, dará a conocer los lineamientos institucionales sobre la materia.

c) No divulgación de información
i. Todos(as) los/las servidores(as) de la SBN estarán sujetos a las cláusulas de confidencialidad establecidas en el tratamiento de la información de su responsabilidad.

ii. En el caso de personal externo, según corresponda al tipo de trabajo que realice, deberá firmar un contrato de no divulgación de la información.

d) Normas de seguridad de la información

i. Es responsabilidad de cada servidor(a) conocer y cumplir la política de seguridad de la información, así como asistir a charlas y/o entrenamientos sobre la materia.
ii. Es obligación de todo(a) servidor(a) informar sobre las vulnerabilidades detectadas y violaciones de seguridad de la información, al CGD. Los mecanismos deberán ser regulados.
iii. Ningún(a) colaborador(a) puede violar los sistemas informáticos y redes de cualquier organización o individuo, ya sea dentro o fuera del horario de trabajo con recursos de la SBN.
iv. El SAPE es el encargado de comunicar a TI, el listado de los/las servidores(as) con licencia mayor o igual a tres (3) meses, para la deshabilitación de la cuenta de usuario(a), salvo solicitud y autorización expresa del/de la Gerente General o Jefe(a) de unidad de organización.

e) Culminación de Vínculo Laboral

El SAPE es el encargado de comunicar a TI, el listado de los/las colaboradores(as) que terminen el vínculo laboral con la SBN, para la deshabilitación de la cuenta de usuario(a) y efectuar la copia de seguridad de la información.

6.3. Para el uso aceptable de los activos

a) Uso de internet

i. El uso de Internet es con fines estrictamente relacionados con las funciones respectivas del cargo asignado al/a la servidor(a), cualquier uso de este servicio para otros propósitos no es aceptable.
ii. El/la usuario(a) deberá considerar las medidas de seguridad que garanticen que su trabajo se llevará a cabo de una manera eficiente y productiva.

b) Uso del correo electrónico institucional

El uso del correo electrónico es solo para temas laborales, no se acepta el uso de correos electrónicos de proveedores gratuitos (gmail, hotmail, yahoo, etc).

c) Traslado de activos fuera de las instalaciones

Los/las usuarios(as) podrán retirar de las instalaciones de la SBN, activos de TI, previa autorización de su inmediato superior y según los formatos establecidos.

d) Uso adecuado de estaciones de trabajo

TI asigna a los/las servidores(as) civiles, en apoyo al cumplimiento de sus labores, una estación de trabajo. Estos equipos son parte del patrimonio de la SBN, y por lo tanto, se debe buscar la mejor forma de utilizarlos, tomando en cuenta aspectos de seguridad físicos y lógicos para su protección.

e) Uso adecuado de la red de datos

i. El TI es la encargada de asignar a cada servidor(a) civil en apoyo al cumplimiento de sus labores, una cuenta de acceso a la red de datos institucional, con la cual el/la servidor(a) civil puede acceder a diferentes elementos que la componen como: servidores de archivos, servidores de bases de datos, impresoras, archivos compartidos, sistemas y aplicaciones Institucionales, entre otros.

ii. Los servidores civiles deben hacer uso de la red y de los servicios relacionados con esta, estrictamente en cumplimiento de las labores institucionales, tomando en consideración la privacidad de otros usuarios y evitar saturar el ancho de banda de la red de la entidad, entre otros argumentos.

f) Uso de equipos portátiles

La SBN asigna equipos tipo portátil, tales como laptops a sus servidores(as) civiles, para facilitarles el cumplimiento de sus labores. Los/las servidores(as) civiles que tengan asignado cualquier equipo tipo portátil deben hacer correcto uso de estos y de la información que contienen.

g) Uso de unidades de red

i. Toda información de carácter institucional debe ser almacenada en las unidades de red provistas por la SBN.

ii. No es de uso aceptable duplicar información en las unidades de red ni almacenar información personal en dichas unidades, por generar un mal uso del almacenamiento institucional.

h) Uso de sistemas de información

i. La SBN, brinda a los/las usuarios(as) sistemas de información para facilitar el cumplimiento de sus labores.
ii. Los/las servidores(as) civiles que tengan asignado el acceso a alguno de los sistemas de información deben hacerlo en correcto uso de la información y datos personales que contienen.

i) Uso de Telefonía

i. El/la servidor(a) debe dar un buen uso al servicio de telefonía IP, entendiendo que es un medio de comunicación para asuntos de la SBN y no personales.
ii. El uso indebido del servicio telefónico será motivo de suspensión del servicio.
iii. Cualquier daño ocasionado al equipo telefónico por mal uso o descuido será responsabilidad del/de la servidor(a).

6.4. <u>Para proveedores</u>

a) Información

i. Toda la información albergada en la red corporativa, de forma estática o circulando a través de ella mediante elementos de comunicación o transmisión, es propiedad de la SBN y tiene el carácter de privada.
ii. De forma rigurosa, todo el personal que accede a los sistemas de información de la SBN y pertenece a una empresa proveedora de servicio debe:
   - Proteger los sistemas de información y redes de comunicaciones contra acceso o uso no autorizado, alteración de operaciones, destrucción, mal uso o sustracción.
   - Proteger la información confidencial, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso o sustracción.
iii. Todo el personal perteneciente a una empresa proveedora de servicio con responsabilidades en áreas de operación o administración de sistemas y redes, debe:
   - Asegurar que la integridad, autenticación, control de acceso, auditoría y registro se contemplan e incorporan al diseñar, implantar y operar los sistemas de información y redes de comunicaciones.
   - Asegurar la confidencialidad de la información almacenada, tanto en formato electrónico como físico.

b) Confidencialidad de la información

i. Todo el personal perteneciente a una empresa proveedora de servicio deberá guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y demás información a la que tengan acceso durante su relación con la SBN por la prestación de servicio de su empresa, tanto en soporte físico como electrónico. Esta obligación continuará vigente tras la extinción del contrato laboral.

ii. En el caso que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información.

c) Contratos

La Gerencia General en coordinación con el CGD y el Sistema Administrativo de Abastecimiento, será la encargada de incluir cláusulas de seguridad y confidencialidad en los contratos con los/las proveedores(as).

d) Concientización

La Oficina de Administración y Finanzas en coordinación con el CDG, brindará a las empresas proveedoras la documentación necesaria relacionada al Sistema de Gestión de Seguridad de la Información de la SBN.

e) Control de acceso físico

i. El personal de empresas proveedoras de servicios deberá portar la tarjeta de identificación en un lugar visible y en forma permanente dentro de las instalaciones de la SBN.

ii. Sólo bajo la vigilancia de personal autorizado, el personal de las empresas proveedoras, puede entrar en las instalaciones del Centro de Datos, y durante un período de tiempo definido.

f) Datos Personales

i. Para garantizar la seguridad de los datos de carácter personal albergados en la SBN, el personal que pertenece a empresas proveedoras de servicio debe observar las siguientes normas de actuación:

- Solo acceder a las áreas establecidas en el alcance de servicio.
- Evitar traer instrumentos que no serán usados en el servicio.

g) Eliminación de derechos de acceso y devolución de activos

Una vez finalizada la relación contractual entre la empresa proveedora de servicios y la SBN, se procederá al retiro de las credenciales de acceso (usuarios, contraseñas, etc.) creadas, siendo Tecnologías de la Información, la encargada del retiro de estas credenciales; de igual forma, la empresa proveedora de servicios tendrá la obligación de entregar los activos de propiedad de la SBN usados durante el servicio contratado.

6.5. Para la identificación y autenticación de usuarios de los recursos tecnológicos

a) Identificación y contraseñas requeridas

i. Antes de tener acceso a cualquier recurso de la red, todos los usuarios deben ser identificados mediante un usuario y contraseña.
ii. El usuario y la contraseña son individuales e intransferibles.
iii. Está prohibido el uso de un nombre de usuario ajeno o facilitar el usuario y su contraseña personal a un tercero.
iv. Los proveedores de servicios y terceras partes que necesiten acceder a una cuenta de usuario de la SBN, deberán ser identificados con el prefijo “prov”, estas cuentas serán solicitadas por el/la Gerente General o Jefe(a) del área usuaria indicando el vínculo y periodo contractual del/de la proveedor(a).

b) Protección de Estaciones de Trabajo

Todas las estaciones de trabajo deben tener una contraseña de ingreso y un protector de pantalla (screensaver) con un tiempo de activación máxima.

c) Largo mínimo y contenido de Contraseña

i. El largo y configuración de la contraseña debe verificarse al momento de crearla o modificarla.
ii. Para usuarios, se debe configurar el estándar de restricciones para una contraseña normal, esta deberá tener una longitud mínima de ocho (8) caracteres alfanuméricos: mayúsculas, minúsculas, números y carácter especial.

d) Contraseñas de los/las usuarios, administradores que gestionen los sistemas, la base de datos, la red interna, y los servidores

Todas las contraseñas de los/las usuarios(as) con un nivel de privilegio de administradores deben ser entregadas en un sobre lacrado al Supervisor de Tecnologías de la Información y la vigencia de dichas contraseñas serán de treinta (30) días calendario.

e) Cambio periódico de las contraseñas

i. Todos los/las usuarios(as) deben cambiar su contraseña con una frecuencia de treinta (30) días.
ii. Las contraseñas no deben ser reutilizadas en el tiempo. Los usuarios(as) no deben construir contraseñas que sean idénticas o similares a las últimas utilizadas.
iii. El archivo de contraseñas históricas debe mantenerse siempre encriptado, en aquellas plataformas donde sea factible.

f) Asignación de contraseñas expiradas y reasignación de contraseñas

i. La contraseña asignada a una nueva cuenta obligará al/a la usuario(a) a cambiarla durante su primera conexión.
ii. La solicitud de cambio de contraseña por olvido, se debe efectuar a TI, previa identificación positiva del/ de la usuario(a) que lo solicita.

g) Almacenamiento de Contraseñas

i. No se deben incorporar contraseñas en el código fuente de las aplicaciones.
ii. No se deben mantener listados de contraseñas en archivos de texto plano. Los archivos con listas de usuarios/contraseñas deben mantenerse encriptados en todo momento.

h) Contraseñas en dispositivos de red

i. Todos los dispositivos de red (routers, firewalls, switches) deben tener contraseñas u otro mecanismo de control de acceso.
ii. Si un dispositivo no posee contraseña de acceso, se debe impedir su administración remota, permitiendo la intervención sólo al personal autorizado y en forma directa (conexión local).

i) Contraseñas por omisión

Toda contraseña por omisión provista por el fabricante de cualquier sistema debe ser reemplazada.

j) Recordatorios de Contraseñas

Queda prohibido anotar las contraseñas de acceso en lugares públicos.

6.6. Para el escritorio y pantalla

a) Escritorios Limpios

i. Toda vez que un/una servidor(a) se ausenta de su lugar de trabajo, debe bloquear su estación de trabajo y guardar en lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.
ii. Si el/la servidor(a) está ubicado(a) cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.
iii. Al finalizar la jornada de trabajo, el/la servidor(a) debe guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno.
iv. Se deben establecer las medidas de control que permitan comprobar el correcto cumplimiento de estas disposiciones.
v. Cuando la información se imprime, esta se debe retirar inmediatamente de las impresoras.

b) Pantallas Limpias

Las estaciones de trabajo y equipos portátiles deben tener aplicado el estándar relativo a protector de pantalla, de forma que se active, ante determinado periodo sin uso.

7. GLOSARIO DE TÉRMINOS

CISO: Oficial de Seguridad de la Información de la Superintendencia Nacional de Bienes Estatales.

CGD: Comité de Gobierno Digital de la Superintendencia Nacional de Bienes Estatales – SBN.

Contraseña: Es una combinación de dígitos que brinda la posibilidad de acceder a un recurso. Sirve como protección y como mecanismo de seguridad.

ISO: Organización Internacional de Normalización. Es una organización que crea estándares internacionales y esta compuesta por diversas organizaciones nacionales de normalización.

ISO 27001: Sistemas de Gestión de la Seguridad de la Información.

NTP: Normas Técnicas Peruanas.

Política: Conjunto de directrices que establecen normas, procedimientos y comportamientos que deben llevar los servidores civiles de la institución.

PEI: Plan Estratégico Institucional.

PESEM: Plan Estratégico Sectorial Multianual.

SBN: Superintendencia Nacional de Bienes Estatales.

Seguridad de la información: Es la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): Consiste en un conjunto de políticas, procedimientos, guías, recursos y actividades asociadas, que son gestionados de manera colectiva por una institución.