SENCICO

Servicio Nacional de Capacitación para la Industria de la Construcción

Resolución de Presidencia Ejecutiva Nº 058 -2020-02.00

Lima, 06 de julio del 2020

VISTO:

El Memorando N° 09-2020-05.00, de fecha 07 de enero de 2020, de la Gerente de la Oficina de Planificación y Presupuesto; y,

CONSIDERANDO:

Que, el Servicio Nacional de Capacitación para la Industria de la Construcción - SENCICO es una Entidad de Tratamiento Especial, adscrita al Ministerio de Vivienda, Construcción y Saneamiento, de acuerdo a lo dispuesto en el artículo 20° de la Ley N° 30156, Ley de Organización y Funciones de dicho Ministerio; cuenta con autonomía administrativa, económica y financiera, de conformidad con lo establecido en su Ley de Organización y Funciones, Decreto Legislativo Nº 147;

Que, los artículos 9° y 16° de la Ley N° 29733, Ley de Protección de Datos Personales y los artículos 3° y 10° de su Reglamento, aprobado por Decreto Supremo N° 003-2013-JUS, establecen que, en atención al principio de seguridad, toda entidad pública, como titular de bancos de datos personales, en el tratamiento de dichos datos debe adoptar las medidas de seguridad que resulten necesarias, a fin de evitar cualquier tratamiento contrario a la Ley o a su Reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o de medio técnico utilizado;

Que, mediante Resolución Ministerial N° 004-2016-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos, 2ª Edición”, en todas las entidades integrantes del Sistema Nacional de Informática;

Que, el 22 de noviembre de 2004, la Gerencia General aprobó las siguientes Directivas: i) Directiva GG-OAF-DI-017-2004, “Seguridad y protección física de los equipos y medios de procesamiento de la información en el SENICCO”; ii) Directiva GG-OAF-DI-018-2004, “Prevención y eliminación de virus informáticos en los equipos de cómputo”; y iii) Directiva GG-OAF-DI-020-2004, “Normas técnicas para la seguridad e integridad de la información que se procesa en el SENCICO”;

Que, por documento del visto, la Gerente de la Oficina de Planificación y Presupuesto remite el proyecto de Directiva DI/PE/OAF-INF/N° 002-2020, “Seguridad Informática de la red del SENCICO”, e Informe Técnico respectivo; para su evaluación y aprobación, en cumplimiento de lo dispuesto en el literal b) del sub numeral 7.3., numeral 7) sobre Disposiciones Específicas de la Directiva PE/OPP-AL/001-2014 “Elaboración y Aprobación de Documentos Normativos”;

Que, siendo necesario actualizar las disposiciones internas mencionadas en el cuarto considerando corresponde contar con un documento de gestión que establezca las normas y lineamientos que aseguren los niveles de protección y control de acceso

a los recursos informáticos dentro de la red del Servicio Nacional de Capacitación para la Industria de la Construcción – SENCICO, para mantener la confidencialidad, integridad y disponibilidad de la información;

De conformidad con lo establecido en el inciso j) del artículo 33° del Estatuto del SENCICO, aprobado con Decreto Supremo N° 032-2001-MTC, modificado por Decreto Supremo N° 004-2006-VIVIENDA y Directiva N° PE/OPP-AL/001-2014 para la "Elaboración y Aprobación de Documentos Normativos del SENCICO";

Con el visto del Asesor en Sistemas e Informática, de la Gerente de la Oficina de Planificación y Presupuesto, del Gerente de la Oficina de Administración y Finanzas, del Asesor Legal y del Gerente General;

SE RESUELVE:

ARTICULO 1º.- Aprobar la Directiva N° DI/PE/OAF-INF/N° 002-2020, "Seguridad Informática de la red del SENCICO", la cual consta de siete (07) numerales, y ocho (8) anexos, que forman parte de la presente resolución.

ARTICULO 2°.- Dejar sin efecto las siguientes Directivas aprobadas por la Gerencia General: i) Directiva GG-OAF-DI-017-2004, "Seguridad y protección física de los equipos y medios de procesamiento de la información en el SENICCO"; ii) Directiva GG-OAF-DI-018-2004, "Prevención y eliminación de virus informáticos en los equipos de cómputo"; y iii) Directiva GG-OAF-DI-020-2004, "Normas técnicas para la seguridad e integridad de la información que se procesa en el SENCICO".

ARTICULO 3°.- Encargar a la Oficina de Administración y Finanzas, que a través del Departamento de Informática, publique la presente resolución y sus anexos en el portal institucional (www.sencigo.gob.pe).

Regístrese y Comuníquese

Ms. Ing. ANA VICTORIA TORRE CARRILLO
Presidenta Ejecutiva

FIRMA DIGITAL

Firmado digitalmente por: TORRE CARRILLO Ana Victoria FAU 20131377810 soft
Motivo: Soy el autor del documento
Fecha: 06/07/2020 16:30:14-0500

Firmado digitalmente por: QUEVEDO DE LA CRUZ Isaias Jesus FAU 20131377810 soft
Motivo: Soy el autor del documento
Fecha: 30/06/2020 16:09:59-0500

SENCICO	**DIRECTIVA**		**DI/PE/OAF-INF/N° 002-2020**	
	TITULO: SEGURIDAD INFORMÁTICA DE LA RED DEL SENCICO			
	Aprobado por:	Presidencia Ejecutiva	Fecha de Aprobación:	06 /07/2020
	Propuesto por:	Departamento de Informática		
	Deja sin Efecto:	GG-OAF-DI-017-2004 Seguridad y Protección Física de los Equipos y Medios de Procesamiento de la información en el SENCICO GG-OAF-DI-018-2004 Prevención y Eliminación de Virus Informáticos en los Equipos de Cómputo GG-OAF-DI-020-2004 Normas Técnicas para la Seguridad e Integridad de la Información que se procesa en el SENCICO	Fecha de Publicación:	06/07/2020

1. OBJETIVO

Establecer las normas y lineamientos que aseguren los niveles de protección y control de acceso a los recursos informáticos dentro de la red del Servicio Nacional de Capacitación para la Industria de la Construcción (en adelante, el SENCICO), para mantener la confidencialidad, integridad y disponibilidad de la información.

2. BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado y sus modificatorias.
- Ley N° 27806, Ley de Transparencia y Acceso a la Información Púbica y sus modificatorias.
- Ley N° 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) y sus modificatorias.
- Ley N° 28716, Ley de Control Interno de las Entidades del Estado.
- Ley N° 29733, Ley de Protección de Datos Personales y sus modificatorias.
- Ley N° 30096, Ley de Delitos Informática y sus modificatorias.
- Decreto Supremo N° 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
- Decreto Supremo Nº 030-2002-PCM, Reglamento de la Ley Marco de Modernización de la Gestión del Estado.
- Decreto Supremo Nº 003-2013-JUS, que aprueba el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales.
- Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital
- Resolución de Contraloría N° 320-2006-CG, que aprueban Normas de Control Interno.
- Resolución Jefatural N° 076-95-INEI, que aprueba la Directiva N° 007-95-INEI-SJI "Recomendaciones Técnicas para la Seguridad e Integridad de la Información que se procesa en la Administración Pública".
- Resolución Jefatural N° 386-2002-INEI, que aprueba la Directiva N° 016-2002-INEI/DTNP, sobre Normas Técnicas para el almacenamiento y respaldo de la información procesada por las entidades de la administración pública.
- Resolución Jefatural N° 088-2003-INEI, que aprueba la Directiva Nº 005-2003-INEI/DTNP, sobre "Normas para el uso del servicio de Correo Electrónico en las Entidades de la Administración Pública".
- Resolución Ministerial N° 073-2004-PCM, que aprueba la “Guía para la Administración Eficiente de Software Legal en la Administración Pública”.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de

Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos, 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

- Resolución Ministerial N° 166-2017-PCM, que modifican el artículo 5 de la R.M. Nº 004-2016-PCM referente al Comité de Gestión de Seguridad de la Información.
- Resolución Ministerial N° 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.
- Resolución Ministerial N° 087-2019-PCM, que aprueban disposiciones sobre conformación y funciones del Comité de Gobierno Digital.
- Resolución de Presidencia Ejecutiva N° 31-2014-02.00, que aprueba la Política del Sistema de Gestión de la Seguridad de la Información del SENCICO.

3. ALCANCE

La presente Directiva es de aplicación para todos los empleados del SENCICO a nivel nacional y terceros (tales como: alumnos, prestadores de servicios, empresas aportantes, entidades del estado, entre otros) que acceden a los recursos de la red del SENCICO, quienes estarán sujetos a los mismos requerimientos de seguridad y tienen las mismas responsabilidades de seguridad de la información.

4. VIGENCIA

Esta directiva entra en vigencia a partir de la emisión de la Resolución que aprueba la misma, y su actualización se realiza en función a los cambios o necesidades que surjan en adelante.

5. GLOSARIO DE TÉRMINOS

5.1 Acuerdo de Confidencialidad:

Es una manifestación de la voluntad entre dos partes encaminada a producir la obligación de guardar y no revelar a terceros información que una de las partes desea proteger, durante la vigencia y después del término de las relaciones contractuales.

5.2 Antimalware:

El antimalware es un software diseñado para prevenir, detectar y remediar infecciones por malware en los dispositivos informáticos individuales y sistemas TI. Este software usa múltiples métodos de detección que permiten encontrar comportamiento sospechoso y sistemas basados en reputación con información sobre el malware existente.

5.3 Catálogo Global:

El Catálogo Global es un repositorio de datos distribuido que contiene una representación parcial de cada objeto de cada dominio en una infraestructura de directorio activo.

5.4 Controlador de Dominio:

Un Controlador de dominio contiene la base de datos de objetos del directorio para un determinado dominio, incluida la información relativa a la seguridad. Además, será responsable de la autenticación de objetos dentro de su ámbito de control.

5.5 Data Center:

Se denomina Data Center o centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización. También se le conoce como centro de cómputo.

5.6 Datos Personales:

Toda información sobre una persona natural que la identifica o la hace identificable a través de los medios que pueden ser razonablemente utilizados.

5.7 Denegación de Servicios (DoS – Denial of Services):

Los ataques de denegación de servicios son intentos malintencionados de degradar seriamente el rendimiento de la red o un sistema llegando al punto de impedir su utilización por parte de usuarios legítimos (disponibilidad). Algunas técnicas de DoS se basan en el envío de paquetes especialmente construidos para explotar alguna vulnerabilidad en el software o en el hardware del sistema produciendo saturación de los flujos de datos y de la red o sobrecarga de procesos en los dispositivos. El ataque se puede dar de muchas formas, pero todas tienen algo en común: utilizan la familia de protocolos TCP/IP para conseguir su propósito.

5.8 Directorio Activo

Es una base de datos jerárquica que proporciona la capacidad de establecer un único inicio de sesión y un repositorio central de información para toda su infraestructura, lo que simplifica ampliamente la administración de usuarios y equipos, proporcionando además la obtención de un acceso mejorado a los recursos en red.

5.9 Disponibilidad

Propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada.

5.10 Dispositivos Móviles

Aparatos de tamaño pequeño, con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, diseñado específicamente para una función, pero que puede llevar a cabo otras funciones más generales, siendo su principal característica la movilidad. Se incluyen en este tipo de dispositivos: laptops, smartphones, tablets o similares.

5.11 Estación de Trabajo:

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

5.12 Equipo de Comunicación

Son los equipos utilizados para proporcionar los servicios de voz, datos y video. Entre estos equipos tenemos a los routers, switches, teléfonos. Etc.

5.13 Firewall:

Un producto de hardware o software, conocido también como cortafuegos, que protege una red de acceso no autorizado permitiendo al mismo tiempo comunicaciones autorizadas.

5.14 Incidente de Seguridad de la Información:

Uno solo o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la institución y amenazar la seguridad de la información.

5.15 Información Crítica o Sensible:

Es toda información clasificada como tal por ley (Ejemplo: Datos de empleados, alumnos, proveedores, etc.) u otra que sea considerada como tal por los procesos del SENCICO, las cuales de verse afectadas en una o en todas sus características (Integridad, Disponibilidad y Confidencialidad) podrían conllevar un impacto negativo de índole legal, económica o de imagen institucional.

5.16 Integridad:

Propiedad de salvaguardar la exactitud y completitud de la información.

5.17 IP (Internet Protocol):

Es el protocolo de la capa de red de la suite TCP/IP (modelo OSI). Es responsable de las comunicaciones extremo a extremo en una red TCP/IP e incluye funciones tales como el direccionamiento, el enrutamiento y la fragmentación.

5.18 LAN (Local Área Network):

Un grupo de computadoras u otros dispositivos que comparten una ubicación geográfica reducida y un medio común, tal como un tipo particular de cable (UTP, coaxial, fibra óptica).

5.19 Malware:

Un término genérico que se refiere a cualquier software que tiene una intención maliciosa, ya sea obvia u oculta; tales como: los virus, gusanos, caballos de troya, rootkits, ransomware, software botnet, etc.

5.20 Memoria USB (Universal Serial Bus):

Es un dispositivo de almacenamiento que utiliza una memoria flash para guardar información. Se le conoce también con el nombre de unidad flash USB, lápiz de memoria, lápiz USB, minidisco duro, unidad de memoria, llave de memoria, pen drive, entre otros.

5.21 Mesa de Servicios TI:

Servicio de soporte informático que brinda el Departamento de Informática a los usuarios de la institución. Cuenta con hardware y software que facilita la resolución de problemas.

5.22 NOC (Network Operations Center):

Es el lugar desde el cual se efectúa la gestión y monitoreo de la red.

5.23 NTP (Network Time Protocol):

Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos.

5.24 Protocolo:

Un conjunto de reglas acordadas y formatos de mensajes para el intercambio de información entre los dispositivos de una red.

5.25 Recursos Informáticos:

Todos aquellos componentes de Hardware y Software que son necesarios para el buen funcionamiento y la optimización del trabajo con computadoras y periféricos, tanto a nivel individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos. Entre los recursos informáticos tenemos a las estaciones de trabajo, impresoras, escáneres, dispositivos móviles, antimalware, firewall, etc.

5.26 Red:

Conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos.

5.27 Seguridad de la Información:

Preservación de la confidencialidad, integridad y disponibilidad de la información, por medio de un conjunto de medidas técnicas, organizativas y legales.

5.28 Seguridad Informática:

Conjunto de medidas técnicas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, pudiendo además abarcar otras propiedades como la autenticidad, la fiabilidad y el no repudio.

5.29 SPAM:

Se llama spam o correo basura a los mensajes no solicitados, no deseados o de remitente desconocido y que son sumamente molestos. Por lo general, las direcciones remitentes son: robadas, compradas, recolectadas en la web o tomadas de cadenas de mail. Muchos de estos mensajes vienen infectados de virus, gusanos y caballos de Troya.

5.30 Spyware:

Es un software malicioso que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario de la computadora.

Un spyware típico se auto instala en el sistema afectado de forma que se ejecuta cada vez que se pone en marcha la computadora utilizando CPU, memoria RAM y reduciendo su performance.

A diferencia de los virus, no se intenta replicar, por lo que funciona como un parásito.

5.31 Super Usuario:

Usuario que posee los más altos privilegios en un determinado sistema o plataforma tecnológica.

5.32 Usuario de Red:

Persona que utiliza los recursos de red con privilegios predefinidos.

5.33 UTM (Unified Threat Management):

Se refiere a una sola solución de seguridad, que ofrece varias funciones de seguridad en un solo punto en la red. Un producto UTM generalmente incluye funciones como antivirus, anti-spyware, anti-spam, firewall de red, prevención y detección de intrusiones, filtrado de contenido y prevención de fugas de información. Algunas unidades también

ofrecen servicios como enrutamiento remoto, traducción de direcciones de red (NAT, network address translation) y compatibilidad para redes privadas virtuales (VPN).

5.34 Virus:

Un tipo de programa malicioso que se replica a sí mismo uniéndose a un archivo ejecutable o al sector de arranque de la computadora y realiza una acción específica, por lo general algún tipo de daño a una hora determinada.

5.35 VPN (Virtual Private Network):

Una técnica para conectar una red desde una ubicación remota usando el Internet como medio de red. Un usuario puede usar los servicios de un proveedor de servicios de Internet (ISP) y conectarse a través de Internet a una red privada en un lugar distante, utilizando un protocolo tal como el Point-to-Point Tunneling Protocol (PPTP) para asegurar el tráfico privado.

5.36 WAN (Wide Area Network):

Una red que abarca una gran área geográfica utilizando conexiones de larga distancia punto a punto, en lugar de los medios de comunicación de red compartida, como ocurre en una red de área local (LAN). Las redes WAN pueden utilizar una variedad de tecnologías de comunicación para sus conexiones, tales como líneas telefónicas alquiladas, líneas RDSI o conexiones DSL. El Internet es el ejemplo más amplio de una WAN.

6. DISPOSICIONES GENERALES

6.1 DE LAS RESPONSABILIDADES

6.1.1. GERENCIA GENERAL

6.1.1.1. Fomentar programas de capacitación y entrenamiento permanente en Seguridad de la Información para los empleados del SENCICO a nivel nacional y terceros autorizados, acuerdo a su función y rol en la Institución, en coordinación con el Departamento de Informática y las dependencias respectivas.

6.1.2. COMITÉ DE GOBIERNO DIGITAL

6.1.2.1. Gestionar la asignación de personal y recursos necesarios para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en sus Planes Operativos Institucionales, Plan Anual de Contrataciones y otros.

6.1.3. OFICINA DE ADMINISTRACIÓN Y FINANZAS

6.1.3.1. Disponer que todos aquellos mencionados en el alcance de la presente directiva firme el Acuerdo de Confidencialidad según el Anexo N° 03: Acuerdo de Confidencialidad.

6.1.3.2. Disponer, a través del Departamento de Recursos Humanos, la inducción a todos aquellos mencionados en el alcance de la presente directiva, sobre las disposiciones contenidas en la misma.

6.1.3.3. Velar por el cumplimiento de la presente Directiva, a través del Departamento de Informática.

6.1.4. DEPARTAMENTO DE RECURSOS HUMANOS

6.1.4.1. Comunicar oportunamente al Departamento de Informática los ceses, renovaciones y traslados de los empleados que trabajan en el SENCICO.

6.1.5. TODAS LAS DEPENDENCIAS

6.1.5.1. Comunicar oportunamente al Departamento de Informática los ceses, renovaciones y traslados de consultores o contratistas temporales que trabajan en el SENCICO.

6.1.6. DEPARTAMENTO DE INFORMÁTICA

6.1.6.1. Administrar la seguridad informática para preservar el hardware, el software y demás infraestructura que soportan las operaciones del SENCICO.

6.1.6.2. Poner en conocimiento de las dependencias competentes los incumplimientos de las disposiciones contenidas en la presente directiva.

6.1.6.3. Instalar y configurar los recursos informáticos.

6.1.6.4. Llevar un inventario de todos los equipos de la infraestructura de TI y seguridad, en donde se registra la ubicación, marca, modelo, detalles propios como: serie, código patrimonial, etc. Por tal motivo, el traslado, manipulación y/o modificación de algunos de los detalles mencionados anteriormente deben ser informados anticipadamente al Departamento de Informática; el cual, previa evaluación de riesgos, aprobará y coordinará las acciones a realizar para garantizar el normal desenvolvimiento de las actividades.

6.1.6.5. El personal de soporte técnico informático es responsable de las actualizaciones del antivirus en las computadoras monousuario (no conectadas a la red).

6.1.6.6. Gestionar las copias de respaldo de la información institucional.

6.1.6.7. Mantener actualizada la relación de usuarios.

6.1.7. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN.

6.1.7.1. Informar al Comité de Gobierno Digital del SENCICO sobre los incidentes de seguridad que sean relevantes y puedan afectar la ejecución de las actividades del SENCICO.

6.1.7.2. Gestionar, monitorear y controlar la implementación del Sistema de Gestión de Seguridad de la Información del SENCICO según la NTP/ISO/IEC 27001:2014 y la NTP/ISO/IEC 17799:2007 EDI.

6.1.7.3. Evaluar el estado de situación del Sistema de Gestión de Seguridad de la Información del SENCICO.

6.1.7.4. Liderar y velar por el desarrollo, implementación, mantenimiento y cumplimiento de políticas y procedimientos para promover la seguridad de la información.

6.1.7.5. Participar en equipos de trabajo de TI para monitorear los cambios en la infraestructura de Tecnologías de Información que pongan en riesgo la seguridad de la información.

6.1.7.6. Gestionar los incidentes de seguridad de la información implementando acciones preventivas y correctivas.

6.1.7.7. Seguimiento del cumplimiento de las medidas correctivas a las observaciones de Auditoría en materia de seguridad de la información.

6.1.7.8. Asesorar en temas de la Seguridad de la Información a todas las unidades orgánicas del SENCICO.

6.1.7.9. Capacitar y sensibilizar a los empleados del SENCICO a nivel nacional y terceros autorizados por el SENCICO, en temas de Seguridad de la Información.

6.1.7.10. Participar y apoyar en la implementación de la Ley de Protección de Datos Personales.

6.1.7.11. Informar trimestralmente al Comité de Gobierno Digital sobre los asuntos relacionados con las labores que realiza y cada vez que la situación lo requiera.

6.1.8. USUARIOS

6.1.8.1. Cumplir con las disposiciones señaladas en la presente directiva, a fin de asegurar la eficacia de las medidas de control sobre los recursos informáticos.

6.1.8.2. Reportar al Departamento de Informática los incidentes que afecten la seguridad de la información.

6.1.8.3. El buen uso de las estaciones de trabajo asignadas.

6.1.8.4. De la seguridad física de los dispositivos móviles que son usados fuera de las instalaciones del SENCICO.

6.1.8.5. Es responsabilidad directa de cada usuario mantener la contraseña en secreto y de uso exclusivo de los empleados del SENCICO a nivel nacional y terceros autorizados.

6.1.8.6. Los empleados del SENCICO a nivel nacional y terceros autorizados que tiene a su cargo computadora monousuario, es responsable de detectar y eliminar las infecciones de malware en este equipo y también en los medios magnéticos u ópticos que utilice. Para tal efecto, utilizará los lineamientos dispuestos por el Departamento de Informática.

6.1.8.7. Es responsabilidad directa de cada usuario apagar los equipos informáticos bajo su custodia al concluir las labores del día, así como bloquear o cerrar la sesión al dejar de usar su computadora.

6.1.9. DEPENDENCIAS ZONALES

6.1.9.1. Velar por el cumplimiento de la presente directiva en su respectiva sede, de la integridad física de los equipos de su sede. Está prohibido el acceso y la manipulación a dichos equipos por parte de los empleados del SENCICO a nivel nacional y terceros que el Departamento de Informática no autorice.

6.1.9.2. Es responsabilidad de las dependencias zonales comunicar oportunamente al Departamento de Informática los ceses, renovaciones y traslados de los empleados y terceros que trabajan en su respectiva zonal.

6.2 DE LA SEGURIDAD DE LOS RECURSOS INFORMÁTICOS

6.2.1 Los recursos informáticos y el uso correcto de la información crítica o sensible del SENCICO permiten el normal desempeño de las actividades de la entidad.

6.2.2 Los cambios en la configuración de los recursos informáticos son realizados previa evaluación del impacto por el Departamento de Informática.

6.2.3 Los empleados del SENCICO a nivel nacional y terceros autorizados a quienes se le ha asignado un dispositivo móvil de propiedad del SENCICO, en caso de robo o extravío debe efectuar el procedimiento para bienes siniestrados contenido en la Directiva OAF N° 02 – 2013 "Procedimiento para el control, responsabilidad y uso de los bienes patrimoniales del SENCICO".

6.3 DE LA SEGURIDAD FÍSICA Y DEL ENTORNO

6.3.1. Los equipos de comunicación que se encuentran instalados en las diferentes Sedes están protegidos con medidas de seguridad conocidas (gabinete cerrado con llave y sistema de alimentación continua de energía).

6.3.2. El sistema de alimentación continua de energía está soportado por pozos con puesta a tierra, tableros de distribución eléctrica independientes y UPS con una autonomía de 60 minutos como mínimo.

6.3.3. Los sistemas de agua y desagüe se encuentran en niveles inferiores con respecto a los ambientes donde se ubican los Data Center, de los cuartos de comunicaciones y los gabinetes de comunicaciones en caso de encontrarse fuera de estos ambientes.

6.3.4. Los equipos y servidores de la infraestructura informática del SENCICO, están ubicados en los Data Center.

6.3.5. Los equipos de comunicación de la infraestructura del SENCICO están ubicados dentro de gabinetes o cuartos de comunicaciones en las diferentes sedes de la Institución.

6.3.6. El Departamento de Informática deberá implementar y actualizar los controles de acceso para el ingreso de los empleados del SENCICO y terceros autorizados al Data Center, así como las medidas de seguridad para la administración de los recursos informáticos y de comunicaciones que se encuentran en el Data Center.

6.3.7. El Data Center cuenta con equipos de aire acondicionado que permiten que los equipos instalados funcionen en las condiciones de temperatura adecuadas.

6.3.8. El Data Center cuenta con sistemas de detección y apagado de incendios.

6.3.9. El Departamento de Informática deberá implementado un sistema de monitoreo automático y/o manual de las condiciones ambientales de temperatura y humedad del Data Center.

6.3.10. El Departamento de Informática deberá contar con un plan de mantenimiento preventivo y correctivo de los equipos de comunicaciones, servidores y estaciones de trabajo para garantizar su disponibilidad e integridad.

6.3.11. El cableado de energía eléctrica y telecomunicaciones que transportan datos/voz/video o respaldan servicios de información frente a interceptaciones o daños se encuentran protegidos.

6.4 DEL CONTROL DE ACCESO A LA RED, SUS SERVICIOS, AL SISTEMA OPERATIVO Y SEGURIDAD DE LOS DATOS

6.4.1. Los dispositivos o recursos de telecomunicaciones para el tratamiento de la información tienen configuradas rutas establecidas (pre-definidas) y dominios lógicos de acceso al sistema, los cuales están segmentados y divididos tomando como premisa el control de acceso a la red y los objetivos principales de la Institución.

6.4.2. Se aplican medidas de control a los dispositivos de la red para la protección y acceso de los mismos y para evitar que usuarios no autorizados puedan modificar las configuraciones establecidas.

6.4.3. Los equipos para servicios de telefonía, videoconferencia y video vigilancia IP están protegidos para garantizar su seguridad.

6.4.4. Todos los dispositivos y aplicaciones que forman parte de la red del SENCICO se sincronizan a una fuente de tiempo confiable y exacto a través del protocolo NTP. Se han configurado 2 fuentes de sincronización de hora. La sincronización de hora es esencial para la investigación de eventos/incidentes que ocurren en la infraestructura.

6.4.5. Se permite la conexión a la red administrativa del SENCICO a los dispositivos móviles de propiedad de la institución, del personal que administra los servicios e infraestructura informática (autorizados por el Departamento de Informática), de terceros (proveedores con contrato vigente) o de visitantes temporales (sólo para el uso de Internet) autorizados por la dependencia en la cual van a realizar los trabajos/visita.

6.4.6. Se permite el acceso de los dispositivos móviles personales de los empleados del SENCICO a nivel nacional y terceros únicamente con la autorización de la Gerencia General. En todos estos casos, el personal técnico del Departamento de Informática revisa estos dispositivos, para realizar el análisis de riesgos respectivo antes de otorgar los accesos solicitados. Los requisitos mínimos para que un dispositivo móvil sea conectado a la red es que tenga su sistema operativo y solución antivirus actualizados.

6.4.7. Se prohíbe la conexión a la red y a los servicios de Internet a cualquier dispositivo móvil cuyo acceso no haya sido otorgado por el Departamento de Informática.

6.4.8. El acceso a los servicios de red de la institución es factible para todos los empleados del SENCICO a nivel nacional y terceros al momento de adquirir vínculo laboral con la institución. El área responsable a la que pertenece el empleado del SENCICO o el tercero autorizado, debe solicitar la creación y el acceso a los servicios y privilegios de la red (correo electrónico, Internet, telefonía IP, sistemas, entre otros) de acuerdo al Anexo N° 04: Instructivo de Gestión de Usuarios.

6.4.9. Para acceder a los recursos de la red, los controladores de dominio autentican a los equipos cuando éstos inician sesión, esta información se encuentra registrada en cada catálogo global del directorio activo, el cual permite el control y autenticación.

6.4.10. La conexión se valida sólo si el usuario ha ingresado todos los datos solicitados: nombre de usuario y contraseña, y se registra en el visor de eventos de los controladores de dominio su intento de ingreso (sea éste exitoso o no).

6.4.11. Se comparten carpetas dentro de la red sólo para fines estrictamente laborales. El usuario que comparta una carpeta en la computadora que le fue asignada se hace responsable de la información contenida en ella y de los privilegios que otorgue a la misma a los demás usuarios de la red.

6.4.12. El acceso remoto a las estaciones de trabajo dentro de la red está permitido sólo al personal del Departamento de Informática. Las excepciones son autorizadas por el Departamento de Informática.

6.4.13. Los sistemas de Información y los recursos de la red del SENCICO están disponibles de lunes a domingo desde las 06:00 hasta las 22:00.

6.4.14. Los accesos a los recursos de la red del SENCICO fuera de los días y horario definidos en 6.4.13, son solicitados al Departamento de Informática con oportunidad a través del formato Anexo N° 01 SGSI-FORM-21: Solicitud de Servicios, indicando los usuarios que requerirán el acceso, el(los) día(s) y el horario en el que asistirán a trabajar.

6.5 DE LAS CONTRASEÑAS Y SEGURIDAD

6.5.1. Las contraseñas representan el factor fundamental de la seguridad de los recursos informáticos, ya que es la primera línea de protección para el usuario y para la red.

6.5.2. El propietario de una cuenta de usuario es el único responsable del uso de la misma, siendo la cuenta de usuario y su contraseña de carácter personal e intransferible. Queda totalmente prohibido compartirlas para ser usadas por terceras personas. Por lo mismo, está prohibido solicitar el reseteo de la contraseña de una cuenta de usuario para ser utilizada por persona distinta al titular, sin importar el sustento (enfermedad repentina, ausencia al trabajo, vacaciones, etc.).

6.6 DE LA GESTION DE CUENTAS Y CLAVES DE SÚPER USUARIO

6.6.1. Por los privilegios que poseen los súper usuarios, se tiene un estricto control para la gestión de estas cuentas y sus respectivas claves de acceso.

6.6.2. No se han configurado más de dos cuentas de súper usuario por cada sistema de información o plataforma tecnológica.

6.6.3. Se han adoptado buenas prácticas de seguridad en la selección y uso de contraseñas de las cuentas de súper usuarios.

6.7 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, VIRUS, SOFTWARE MALICIOSO Y SIMILARES

6.7.1. El Departamento de Información deberá contar con soluciones antivirus, antispyware, anti spam, filtro de contenido, firewalls, administración unificada de amenazas (UTMs) y similares para garantizar la seguridad informática de los equipos de cómputo que forman parte esencial del patrimonio de la institución a nivel de todas las sedes del SENCICO.

6.8 DE LA SEGURIDAD EN LA TRANSMISIÓN DE VOZ Y DATOS

6.8.1. El Departamento de Informática en coordinación con los proveedores del servicio de transmisión de voz y datos de la red del SENCICO, garantizan la seguridad en la transmisión sin interrupciones a través de los medios de enlace.

6.8.2. Los dispositivos de red que interconectan la infraestructura tecnológica a nivel nacional están configurados con rutas establecidas (pre-definidas) y dominios lógicos que encaminan el tráfico de la red y garantizan que los datos lleguen a su destino final.

7. DISPOSICIONES ESPECÍFICAS

7.1 DE LA SEGURIDAD DE LOS RECURSOS INFORMÁTICOS

7.1.1. Para el acceso físico y/o lógico se establecen las siguientes medidas:

7.1.1.1. **En las áreas y el entorno donde se encuentran**: Son áreas seguras y los entornos están protegidos por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada y acceso apropiados.

7.1.1.2. **Seguridad de los equipos**: Los equipos están protegidos para evitar pérdidas, daños o que se comprometa su seguridad con el fin de minimizar los riesgos de interrupciones en las actividades de la institución.

7.1.1.3. **Control de acceso:** Se controla el acceso a la información en base a los requisitos de seguridad y los requerimientos de función, con perfiles de acceso estandarizados según el tipo de actividad que realiza el usuario.

7.1.1.4. **Gestión de accesos de usuarios**: Se supervisan y monitorean los accesos para evitar accesos no autorizados a los sistemas de información.

7.1.1.5. **Control de acceso a la red**: Se controla el acceso a los servicios, así como a las redes internas y externas de forma tal que el acceso a la red y a sus servicios no comprometa la seguridad de los mismos.

7.1.1.6. **Control de acceso al sistema operativo**: Para evitar accesos no autorizados a los computadores se utilizan las prestaciones de seguridad del sistema operativo.

7.1.1.7. **Control en la identificación y autenticación de usuario**: se cuenta con un identificador único y exclusivo para uso personal, a fin de registrar y auditar las actividades de cada usuario.

7.1.2. Los equipos de cómputo y servidores, son para uso exclusivo de las actividades laborales asignadas a cada trabajador. Éstos no son usados para fines comerciales o actividades no relacionadas al SENCICO.

7.1.3. Los empleados del SENCICO a nivel nacional y terceros autorizados a quienes se le han asignado un dispositivo móvil, debe proteger el equipo de accesos y usos no autorizados.

7.1.4. Ningún trabajador debe intentar vulnerar la seguridad de la red del SENCICO, limitándose al uso de los accesos otorgados.

7.1.5. El software protegido por derechos de autor no debe ser copiado en ningún tipo de medio magnético, óptico u otra índole. No está autorizada:

- La copia de software de propiedad del SENCICO. Esto significa que el software debe ser copiado solamente para fines de respaldo y sólo en caso de estar permitido por la licencia del software.
- La instalación de software en equipos del SENCICO que no haya sido autorizado por el Departamento de Informática.
- La copia de software protegido por derechos de autor usando los recursos informáticos del SENCICO. Estas copias sólo pueden ser realizadas por el personal del Departamento de Informática, previa validación de las condiciones de licenciamiento.

7.2 DE LA SEGURIDAD FÍSICA Y DEL ENTORNO

7.2.1. DE LAS ESTACIONES DE TRABAJO Y DE LOS DISPOSITIVOS MÓVILES

7.2.1.1 La ubicación actual de la estación de trabajo dentro de un ambiente determinado, es definido sobre un plano de distribución. Por lo tanto, su ubicación forma parte de la implementación de cableado estructurado de red, es por ello que está prohibido reubicarse y/o mudarse de la misma sin la debida coordinación y/o autorización del Departamento de Informática.

7.2.1.2 Para el uso de los dispositivos móviles se deben tomar las siguientes medidas de seguridad:

- Los dispositivos móviles utilizados en espacios públicos deben estar al alcance de la persona que lo tiene asignado.
- Acceder solamente a redes seguras.
- Para su correcto transporte, debe tener el equipaje de mano adecuado.
- Se siguen las instrucciones del fabricante tales como la protección por exposición a campos electromagnéticos, temperatura ambiental permitida, entre otros.
- Velar por la seguridad física del dispositivo móvil de propiedad del SENCICO que es usado fuera de sus instalaciones y es conectado a una red inalámbrica o alámbrica que no es administrada por la institución.

7.2.2. DE LOS EQUIPOS DE COMUNICACIÓN QUE SE UBICAN EN EL DATA CENTER

7.2.2.1 Para la administración de los recursos informáticos y de comunicaciones que se encuentran en el Data Center, el Departamento de Informática implementará medidas de seguridad, tales como: sistema de control de accesos, servicio de alimentación ininterrumpida, flujo de alimentación eléctrica estabilizada, sistema de refrigeración, así como el control del ingreso sólo a los empleados del SENCICO o a terceros autorizados.

7.2.2.2 El ingreso de los empleados del SENCICO a nivel nacional y terceros autorizados al Data Center se realiza de acuerdo al Anexo N° 05: Instructivo de Seguridad y Correcto Uso de las Instalaciones de Procesamiento de la Información.

Se cuenta con tres tipos de accesos:

a. Acceso Directo: Se otorga a los empleados del SENCICO a nivel nacional y terceros autorizados que por naturaleza de sus funciones tiene acceso permanente a las instalaciones del Data Center y no requiere autorización expresa. Ejemplo: personal del NOC.
b. Acceso Autorizado: Se otorga a los empleados del SENCICO a nivel nacional y terceros autorizados que requiere ingresar al Data Center eventualmente. Este personal debe figurar en la lista autorizada y debe registrar su ingreso en la bitácora de control de acceso al Data Center – Anexo N° 02: SGSI-FORM-37 "Bitácora de Acceso al Data Center". Ejemplo: DBA, responsable del Departamento de Informática.
c. Acceso Especial: Se otorga excepcionalmente al empleado del SENCICO y/o tercero autorizado, por lo tanto requiere autorización expresa del responsable del Departamento de Informática. A su vez debe registrar su ingreso en la bitácora de control de acceso al Data Center – Anexo N° 02: SGSI-FORM-37 "Bitácora de Acceso al Data Center".

7.2.2.3 El personal del NOC es el encargado de apoyar el registro, supervisar, custodiar y asistir al visitante autorizado de ingresar al Data Center. En él recae la responsabilidad del actuar del visitante dentro del área en mención. Asimismo, la presencia del personal del NOC debe ser permanente, a fin de evitar cualquier eventualidad que interrumpa el normal funcionamiento de los recursos y equipos ubicados en el Data Center.

7.2.2.4 El Departamento de Informática deberá contar con un plan de mantenimiento preventivo y correctivo de los equipos de comunicaciones y servidores para garantizar su disponibilidad e integridad.

7.2.3 DE LOS EQUIPOS INSTALADOS EN LOS GABINETES DE COMUNICACIONES DE CADA PISO EN LAS SEDES DEL SENCICO

7.2.3.1 Estos equipos se encuentran resguardados por medios de protección conocidos (gabinete cerrado con llave y sistema de alimentación ininterrumpida).

7.2.3.2 El cableado estructurado de voz, video y datos se encuentra alineado a los estándares y normas de cableado vigentes en la región, asegurando la integridad y disponibilidad de la transmisión.

7.3 DEL CONTROL DE ACCESO A LA RED, SUS SERVICIOS, AL SISTEMA OPERATIVO Y SEGURIDAD DE LOS DATOS

7.3.1 DEL CONTROL DE ACCESO A LA RED

7.3.1.1 Para la creación de una cuenta de usuario se utiliza el siguiente estándar: Primera letra del nombre de pila del usuario, seguido inmediatamente del apellido paterno. En caso de existir dos

construcciones de cuenta de usuario similares, se añadirán progresivamente las letras del apellido materno hasta establecer la diferencia.

7.3.1.2 Al crearse una cuenta, se establece una contraseña temporal, la cual es forzada a cambiarse por el sistema luego del primer inicio de sesión. El usuario elige la contraseña con el formato y sintaxis indicados en esta directiva y asume la responsabilidad sobre la inviolabilidad de su contraseña desde ese momento y cada vez que la renueve.

7.3.1.3 Se han establecidos políticas de acceso por perfiles, restringiendo la instalación de software no autorizado, el acceso al panel de control y otras opciones de configuración de las computadoras. Siempre que se requiera para el normal cumplimiento de sus funciones, se puede solicitar excepciones temporales a dichas restricciones, las que serán solicitadas por el responsable del área a la que pertenece el usuario mediante el formato Anexo N° 01: SGSI-FORM-21 "Solicitud de Servicios". El personal del Departamento de Informática, por la naturaleza de sus funciones, está exceptuado de estas restricciones, así como los Gerentes.

7.3.1.4 Se realizan verificaciones periódicas de los privilegios asignados a los usuarios a fin de garantizar su idoneidad.

7.3.1.5 Los registros de eventos se realizan guardando los siguientes parámetros:

- Identificación del usuario.
- Fecha y hora de conexión y desconexión.
- Identificación de la estación de trabajo (nombre/número IP).
- Registro de los intentos aceptados y rechazados de acceso a la red, aplicaciones/base de datos y otros recursos.

7.3.1.6 Se aplican medidas de protección para los dispositivos de la red LAN/WAN para el acceso a los mismos y evitar que los usuarios no autorizados modifiquen las configuraciones establecidas.

7.3.1.7 La conexión a la red LAN está limitado a un dispositivo físico por usuario. De requerir se amplíen la cantidad de dispositivos físicos de usuario, el responsable del área deberá solicitarlo a través de un memorando indicando la necesidad al Departamento de Informática, el mismo dispondrá la evaluación y disponibilidad del servicio y de ser el caso se realizará la habilitación del dispositivo.

7.3.1.8 Está prohibido conectar dentro de las instalaciones del SENCICO cualquier equipo informático sin tener la autorización del Departamento de Informática.

7.3.1.9 Para garantizar la confidencialidad de la información en las comunicaciones en los principales servidores de aplicaciones se utilizan certificados digitales.

7.3.1.10 Para el acceso a la red de los dispositivos móviles de contratistas y visitantes, la solicitud de acceso la realiza el área que requiere el

servicio a través del formato Anexo N° 01: SGSI-FORM-21" Solicitud de Servicios", indicando el motivo de la solicitud, los trabajos que se realizarán y el tiempo de permanencia del proveedor/visitante. Previa evaluación de riesgos, el Departamento de Informática atiende la solicitud. Una vez otorgados los permisos y accesos correspondientes, los cuales son temporales, la dependencia solicitante es responsable del buen uso de los accesos/servicios otorgados a estos dispositivos.

7.3.1.11 Se permite el acceso remoto a los servicios de la red vía VPN (Virtual Private Network), gestionado desde la solución de Seguridad Perimetral, en la cual los datos y la información viajan sobre canales de acceso seguros. Se autoriza el acceso remoto por VPN (por un tiempo determinado) exclusivamente para labores de administración de sistemas, aplicaciones y servicios críticos de la Institución.

7.3.1.12 Para dar de baja a un usuario a quien se otorgó una cuenta con acceso a los recursos de la red del SENCICO, se debe solicitar la eliminación de las cuentas de acuerdo a lo dispuesto en el Anexo N° 04: Instructivo de Gestión de Usuarios.

7.3.1.13 El Departamento de Informática beberá tomar las medidas necesarias para que el acceso al código fuente de los programas desarrollados en el SENCICO esté debidamente protegido.

7.3.2 DEL CONTROL DE ACCESO AL SISTEMA OPERATIVO

7.3.2.1 El Departamento de Informática beberá implementar un control de la descripción y ubicación física de cada usuario, información que está registrada en cada catálogo global del directorio activo. Los controladores de dominio autentican a los equipos cuando éstos inician una sesión e ingresan a la red del SENCICO. Este control y autenticación está también asociado a su dirección lógica o IP, con esta información se puede identificar la ubicación física de cada equipo a nivel nacional.

7.3.2.2 Todo usuario tiene una cuenta de usuario que lo identifica. Cada cuenta de usuario es única y cumple con el formato y sintaxis mencionados en el numeral 7.3.1.1. La excepción corresponde a equipos utilizados para funciones específicas, para los que se definen cuentas genéricas que identifican la función (ejemplo: matrícula, visita zonal, etc.) y que asocia cada cuenta a un único perfil de usuario; cada perfil muestra en el escritorio del computador solamente los íconos de las aplicaciones requeridas para cada función. Estas cuentas de dominio no tienen asociadas direcciones de correo electrónico, pues para ello se requieren usuarios personalizados.

7.3.2.3 El usuario responsable de la estación de trabajo debe bloquear la misma cuando por causa laboral o extra laboral está en la necesidad imperiosa de ausentarse momentáneamente de su puesto de trabajo. Esto impide tanto el acceso no autorizado al sistema, como a las aplicaciones. El usuario que no deje bloqueado su computador al ausentarse, será responsable por el uso no autorizado del equipo, de la red o de las aplicaciones instaladas. En el caso de las computadoras con

sistema operativo Windows 7 en adelante, el bloqueo de la estación de trabajo se realiza presionando simultáneamente las teclas “Windows” y “L”.

Por política en la red del SENCICO, las estaciones de trabajo se bloquean automáticamente luego de 10 minutos de inactividad.

7.3.2.4 Se prohíbe el almacenamiento de archivos de música y video ajenos a las actividades y funciones asignadas a los empleados del SENCICO y terceros autorizados; así como compartirlos a través de la red, pues ponen en riesgo la performance y seguridad de la misma. El Departamento de Informática está facultado a tomar las medidas preventivas y correctivas necesarias para mitigar o eliminar este riesgo.

7.3.2.5 Todos los dispositivos móviles de propiedad del SENCICO, cuentan con una contraseña de protección para acceso al dispositivo como mínimo, y se activan las opciones de bloqueo automático en caso de inactividad.

7.3.3 DE LA SEGURIDAD DE LOS DATOS

7.3.3.1 Para garantizar la confidencialidad se aplica un sistema de autenticación de usuarios registrados en una base de datos a la cual se aplican las siguientes medidas de protección:

- Contraseñas no menores de 8 caracteres.
- Contraseñas encriptadas.
- Formato y sintaxis de la contraseña predefinidos.
- Periodo de expiración de la sesión.
- Tiempo de caducidad de contraseñas.
- Acceso de las cuentas por roles predefinidos.
- Número de intentos fallidos de ingreso a la red permitidos.

7.3.3.2 Para la integridad de la información, el Departamento de Informática deberá implementar accesos y políticas de acceso definidos de acuerdo a los perfiles de usuario.

7.3.3.3 Para garantizar la disponibilidad de la información que se encuentra en los servidores de base de datos, de las aplicaciones y de los medios de comunicación, el Departamento de Informática deberá implementar mecanismos de seguridad para el acceso. Asimismo, los sistemas de comunicación se deberá contar enlaces de respaldo, complementándose con la inclusión de equipos de autonomía eléctrica (UPS) para soportar los equipos de comunicaciones y a los servidores.

7.3.3.4 Los accesos a los servidores y a las estaciones de trabajo sólo se realizan mediante la autenticación.

7.3.3.5 Para el respaldo y restauración de la información del SENCICO se siguen los lineamientos especificados en el Anexo N° 06: Instructivo de Respaldo y Restauración, Anexo N° 07: Instructivo de Traslado de Cintas de Respaldo y Anexo N° 08: Instructivo de Recuperación de Cintas de Respaldo.

7.3.3.6 Toda la información de los dispositivos móviles se borra en forma segura cuando éstos se asignan a otros usuarios o bien son dados de

baja.

7.3.3.7 Las instalaciones de desarrollo, prueba y operación se separan con el fin de reducir el riesgo de acceso no autorizado o cambios en el sistema operacional para el procesamiento de información del SENCICO.

7.3.3.8 Para la prueba de las aplicaciones del SENCICO, se preparan datos de comprobación (set de pruebas) en donde se contemplan todas las entradas correctas y erradas, verificándose las salidas generadas con los resultados previstos.

7.3.3.9 La información más sensible del SENCICO no se almacena en dispositivos móviles, aunque éstos estén cifrados.

7.3.3.10 Las políticas de privacidad publicadas en los sitios web del SENCICO desde donde se recogen datos personales, son fácilmente accesibles e identificables.

7.4 DE LAS CONTRASEÑAS Y SU SEGURIDAD

7.4.1 Como parte de la política de seguridad del SENCICO, el sistema de seguridad solicitará automáticamente al usuario el cambio de contraseña cada 45 días. También se recomienda cambiar las contraseñas siempre que el usuario sospeche que la seguridad de su contraseña pueda estar comprometida o vulnerada, lo cual es informado al Departamento de Informática para la evaluación correspondiente.

7.4.2 El formato y sintaxis de cada contraseña queda establecido bajo los siguientes lineamientos de formato, número de caracteres y tiempo de vida:

- Longitud mínima de 8 caracteres.
- Combinación mínima obligatoria de letras mayúsculas, letras minúsculas, números y caracteres especiales.
- Vigencia de 45 días, al término de los cuales se forzará el cambio de contraseña, no pudiendo repetir las 12 últimas.

7.4.3 Para casos donde se requiera cambiar una contraseña por pérdida u olvido de la misma, el usuario debe solicitarlo de forma personal a la Mesa de Servicios de TI del Departamento de Informática, quienes deben reconfirmar con el usuario solicitante el pedido.

7.4.4 Las contraseñas no deben ser divulgadas o escritas en notas, documentos u otros medios escritos, incluyendo conversaciones telefónicas.

7.4.5 Las contraseñas no deben ser palabras comunes o simples variaciones del nombre del trabajador, usuario, nombre de la computadora, servidor o empresa. Por ejemplo, una contraseña fuerte puede ser: X6g&Ws5y8

7.4.6 Durante el proceso de autenticación ante el sistema, el usuario tiene cuatro intentos para ingresar su contraseña correcta. Si en los 04 intentos ingresa una contraseña incorrecta, la cuenta se bloquea automáticamente. Para volver a activar dicha cuenta deberá ponerse en contacto con Mesa de Servicios de TI para el desbloqueo correspondiente.

7.4.7 Todas las computadoras de la red del SENCICO usan un protector de pantalla institucional que se activa automáticamente luego de 10 minutos de inactividad.

Una vez que el protector de pantalla se active, cada usuario deberá nuevamente autenticarse para volver a tener acceso al sistema.

7.4.8 Para los casos de las dependencias que se conectan mediante accesos remotos a la red a través de la WAN, el usuario realiza doble autenticación; una para establecer el enlace privado con SENCICO y la otra, ya estando dentro de la red, se volverá a autenticar como usuario autorizado de un sistema en particular. Por ejemplo: como usuario de los sistemas SAIS, SIS u otro servicio.

7.4.9 Ante situaciones de sustracción o pérdida de información del equipo de un usuario, causados por la violación de la cuenta de usuario debido a una pobre definición o un mal uso de la contraseña, el usuario es responsable por los daños que pueda causar este hecho a los recursos informáticos del SENCICO. El incidente es evaluado por el Departamento de Informática y luego se comunica a la dependencia competente para su evaluación y adopción de las acciones disciplinarias correspondientes.

7.5 DE LAS GESTION DE CUENTAS Y CONTRASEÑAS DE SÚPER USUARIO

7.5.1 DE LA ASIGNACION DE CUENTAS DE SUPER USUARIO

7.5.1.1 Las solicitudes de creación, modificación y/o eliminación de cuentas de súper usuario deben ser solicitadas vía el formato Anexo N°01 SGSI-FORM-21: Solicitud de Servicios.

7.5.1.2 El Administrador del Sistema o plataforma tecnológica registra las acciones de creación, modificación y/o eliminación de las cuentas de súper usuario, indicando lo siguiente:

- Plataforma tecnológica o sistema de información asociado.
- Acción realizada (creación, modificación, eliminación o contingencia).
- Autorización de la acción.
- Nombre del usuario.
- Cuenta de usuario relacionada.
- Privilegios asignados.
- Fecha de expiración.

7.5.2 DEL RESGUARDO DE CONTRASEÑAS DE LAS CUENTAS DE SUPER USUARIO

7.5.2.1 Las contraseñas de las cuentas de súper usuario son guardadas en sobres sellados y lacrados en la caja fuerte, el contenido de cada sobre debe indicar:

- Plataforma tecnológica o sistema de información asociado.
- Nombre de usuario.
- Contraseña.
- Ubicación lógica del recurso: IP, URL, UNC, esquema, etc.
- Fecha en que se guardó el sobre.

7.5.2.2 Las cuentas de súper usuario no expiran.

7.5.2.3 Los sobres que contienen las credenciales de las cuentas de súper usuario son guardados en la caja fuerte del Departamento de

Informática.

7.5.2.4 Los cambios de contraseña de súper usuario se efectúan en los siguientes casos:

- Cuando se sospecha o exista un mínimo indicio de que se ha vulnerado la confidencialidad de ésta.
- Cuando la contraseña ha sido creada por terceros y los servicios pasan a la administración del SENCICO.
- Cuando es usado por contingencia.

7.5.2.5 Las contraseñas de súper usuario tienen como mínimo las siguientes características:

- Longitud: Ocho caracteres como mínimo.
- Están compuestas por letras mayúsculas, minúsculas, números y caracteres especiales.
- No incluyen caracteres iguales consecutivos.
- Se controla el histórico de 12 contraseñas.

7.5.3 DE LA CONTINGENCIA EN EL MANEJO DE LAS CONTRASEÑAS DE CUENTAS DE SUPER USUARIO

7.5.3.1 Se cuentan con sobres lacrados con las credenciales de las cuentas de súper usuario para ser usadas en caso de contingencia, de ser necesario acceder a la plataforma de tecnología y/o los sistemas de información del SENCICO con dichas cuentas y no esté disponible ninguna persona con estos privilegios o se requiera mayor acceso.

7.5.3.2 En casos de contingencia se retira el sobre correspondiente por parte del personal autorizado para cubrir la contingencia, verificando que existan las autorizaciones correspondientes por parte de los propietarios de la información/sistema/plataforma tecnológica.

7.5.3.3 Una vez superada la contingencia, se gestiona el cambio de contraseña según lo indicado en el numeral 7.5.1 y 7.5.2.

7.5.3.4 El custodio de la caja fuerte lleva un registro documentando de la utilización de las contraseñas y motivo por el cual se necesitó su uso.

7.6 DE LA PROTECCIÓN CONTRA ATAQUES INFORMATICOS, MALWARE Y SIMILARES

7.6.1 DE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS

7.6.1.1 Para la protección contra ataques informáticos externos, el Departamento de Informática deberá implementar equipos de seguridad perimetral de alto rendimiento y en alta disponibilidad como son: Firewalls, IPS/IDS, UTMs (administrador unificado de amenazas) y similares. Estos equipos de seguridad constituyen el primer frente de protección de la red ante los ataques informáticos provenientes de la red pública Internet.

7.6.1.2 Los firewalls restringen los accesos externos a los servicios y aplicaciones web que publica el SENCICO. Estos dispositivos se encargan de aislar la red Interna de la red pública Internet y crear zonas de seguridad. Se han creado reglas de acceso que permiten abrir o cerrar puertos de servicio, habilitar o

bloquear hosts de origen y destino, trasladar direcciones IP públicas a direcciones IP internas de la red del SENCICO y viceversa, así como garantizar la disponibilidad de los servicios que la institución pública en Internet.

7.6.1.3 Los sistemas de prevención de intrusiones (IPS/IDS) detectan y evitan el ingreso de tráfico malicioso e indeseado a la red proveniente de Internet, estos sistemas poseen una base de datos de firmas de ataques conocidos de red y de aplicación, además protegen a la red de ataques de denegación de servicio (DoS).

7.6.1.4 Para la administración de los equipos de seguridad perimetral se cuentan con consolas que gestionan las políticas de seguridad y en las que se han configurado reglas de acceso definidas para cada uno de estos equipos. También se cuenta con servidores/appliances repositorios de logs, donde se registran los accesos y eventos que son generados por cada uno de los equipos de seguridad implementadas. Estos registros de accesos y eventos se almacenan por un periodo de 6 meses y cuentan con copias de respaldo mensuales en cintas magnéticas.

7.6.1.5 El acceso a las herramientas para el monitoreo y administración de la red se realizan a través de hosts de confianza.

7.6.2 DE LA PROTECCIÓN CONTRA MALWARE

7.6.2.1 El antimalware instalado es un software corporativo compuesto por módulos que protegen las estaciones de trabajo y los servidores en tiempo real y que forma parte de la solución de seguridad informática del SENCICO. La gestión de la suite se realiza de manera centralizada mediante una consola web.

7.6.2.2 La consola web centralizada gestiona simultáneamente los siguientes niveles de protección:

- **Nivel equipos (estaciones de trabajo y servidores):** Consta de un software para estaciones de trabajo y servidores, el cual cuenta con un agente que se enlaza a la consola centralizada antimalware, encargada de la actualización permanente, tanto a nivel de firmas como a nivel del motor de búsqueda. Adicionalmente, la consola antimalware permite generar reportes de incidentes con virus, spyware, adware y similares, además de mantener un reporte del estado de actualización de toda la infraestructura.
- **Nivel de Internet y correo electrónico:** Para protección del cliente de correo electrónico realizando una inspección a cada uno de los mensajes recibidos y para minimizar el riesgo del acceso web a sitios fraudulentos/maliciosos que pongan en riesgo la integridad de la información del SENCICO.

7.6.2.3 El servicio de correo electrónico, a través de múltiples motores antimalware, ofrece protección multicapa que está diseñado para capturar todo el malware conocido. Todos los mensajes transportados a través del servicio se analizan en busca de malware (virus y software espía). Se envían notificaciones a los administradores cuando se elimina un mensaje infectado y no entregado.

7.6.2.4 El uso de los puertos USB de una estación de trabajo está restringido por el software antimalware como medida de prevención para asegurar la integridad

y disponibilidad de la información del SENCICO, pues a través de estos dispositivos se podrían causar infecciones por malware en la estación de trabajo y luego propagarse por toda la red. Además, se evita la fuga y pérdida de la información por medio de estos dispositivos.

7.6.2.5 En caso se requiera la habilitación de los puertos USB en modo lectura solamente, para algún usuario por la naturaleza de sus funciones, el área en la cual colabora el usuario debe solicitar a través del formato Anexo N° 01: SGSI-FORM-21 Solicitud de Servicios, la habilitación correspondiente, en el campo "Descripción del Servicio" indica "Habilitación de puerto USB" junto con la justificación de la necesidad. El Departamento de Informática, previa evaluación de riesgos, atiende dicho requerimiento. Cuando se detecte una infección o ataque en progreso, originado por el uso de dispositivos USB, se procederá a revocar el permiso correspondiente.

7.6.2.6 Los dispositivos móviles de propiedad del SENCICO deberá contar con antimalware, anti spam, firewall personal y mecanismos antirrobo, dependiendo del tipo de dispositivo.

7.6.2.7 El usuario con permiso de acceso de solo lectura a los puertos USB de su estación de trabajo, es responsable por las infecciones de malware que pueda causar al ejecutar archivos infectados contenidos en la memoria externa. El incidente será evaluado por el Departamento de Informática y de ser el caso, lo comunicará a las dependencias competentes para la adopción de las medidas disciplinarias correspondientes.

7.6.2.8 El servicio de correo electrónico deberá contar con capacidades de filtrado de malware y spam que ayudan a proteger los mensajes entrantes y salientes de software malicioso, así como también del correo no deseado. Estas capacidades están habilitadas de forma predeterminada, sin embargo, los administradores del servicio de correo pueden realizar personalizaciones de filtrados específicos en la consola de administración del correo electrónico para mejorar los niveles de seguridad.

7.6.2.9 El servicio de correo electrónico institucional cuenta con la opción de creación de listas blancas (remitentes/destinatarios permitidos) y listas negras (remitentes/destinatarios prohibidos).

7.6.2.10 Para restringir la navegación por páginas web fraudulentas y para mitigar el riesgo de infecciones por descarga de archivos y software de dudosa procedencia disponible en internet el SENCICO deberá contar con opciones de filtro de contenido web en los equipos de seguridad perimetral y en el software antimalware. Esto permite la optimización del consumo del ancho de banda de acceso a Internet para evitar que se afecte la disponibilidad de los servicios de la red Internet.

7.6.2.11 Está prohibida la descarga de archivos y/o programas (software gratuito) de los tipos ejecutables (*.exe, *.msi, *.dll, etc.), comprimidos (*.zip,*.rar , etc.), archivos de música y video en todos sus formatos (*.mp3, *.wav , *.mp4, etc.), entre otros, pues pueden contener malware, lo cual puede afectar la seguridad de la información de la Institución. En caso se requiera algún programa del tipo gratuito, deberá ser solicitado al Departamento de Informática a través del

formato Anexo N° 01: SGSI-FORM-21: Solicitud de Servicios especificando el motivo de la necesidad y en qué computadora(s) será(n) instalado(s). Previa evaluación de riesgos y las condiciones del licenciamiento, el Departamento de Informática podrá atender el requerimiento.

7.6.2.12 En caso se detecta en una estación de trabajo una infección por malware o propagación en progreso, el personal del Departamento de Informática está facultado a tomar el control físico o remoto del equipo en cuestión a fin de controlar y mitigar los efectos del malware. En los casos más graves, el equipo será desconectado físicamente de la red hasta eliminar el malware.

7.7 DE LA SEGURIDAD EN LA TRANSMISIÓN DE DATOS Y DOCUMENTOS ELECTRÓNICOS

7.7.1 La transmisión de datos, archivos y documentos electrónicos está garantizada por las medidas de seguridad propias de la gestión de la seguridad de la red que se indica en la presente directiva, la transmisión se realiza a través de la red privada y la red pública.

7.7.2 En la red privada se transmiten datos, archivos y documentos electrónicos a los servidores de aplicaciones, servidores de bases de datos, servidores de almacenamiento y a las estaciones de trabajo de las diferentes dependencias del SENCICO.

7.7.3 En la red pública se ofrecen los servicios de registros y consultas de datos que brinda el SENCICO a terceras partes, tales como: alumnos, empresas aportantes, entidades del estado, entre otros.

7.7.4 La transmisión libre de interceptaciones entre las estaciones emisoras y receptoras, está garantizada por el uso de certificados digitales, controles de accesos, políticas de grupo y perfiles de usuario entre otros mecanismos contemplados en la presente directiva.

7.7.5 Para las operaciones de transferencias de los registros electrónicos, archivos, datos, etc., el sistema automáticamente genera archivos de bitácora (log files) y pistas de auditoría (audit trails) donde se registran la fecha y hora de las operaciones efectuadas, además de otros datos que permiten efectuar la trazabilidad correspondiente.

ANEXOS

ANEXO N° 01: SGSI-FORM-21 Solicitud de Servicios.
ANEXO N° 02: SGSI-FORM-37 Bitácora de Acceso al Data Center.
ANEXO N° 03: Acuerdo de Confidencialidad.
ANEXO N° 04: Instructivo de Gestión de Usuarios.
ANEXO N° 05: Instructivo de Seguridad y Correcto Uso de las Instalaciones de Procesamiento de la Información.
ANEXO N° 06: Instructivo de Respaldo y Restauración.
ANEXO N° 07: Instructivo de Traslado de Cintas de Respaldo.
ANEXO N° 08: Instructivo de Recuperación de Cintas de Respaldo.

ANEXO N° 01
SGSI-FORM-21 SOLICITUD DE SERVICIOS

SENCICO	**FORMATO**		CÓDIGO: SGSI-FORM-21
	TITULO: SOLICITUD DE SERVICIOS		
	Aprobado por:		Fecha Aprobación:
	Reemplaza a:	N° Páginas 23	Fecha Publicación:

Fecha:

Usuario:

Dependencia:

- ☐ Presidencia del Consejo Directivo
- ☐ Control Interno
- ☐ *Gerencia General*
- ☐ Asesoría Legal
- ☐ Desarrollo , Mantenimiento e Infraestructura
- ☐ Laboratorio de Ensayo de Materiales
- ☐ Oficina de Administración y Finanzas
  - ☐ Departamento de Contabilidad
  - ☐ Departamento de Tesorería
  - ☐ Departamento de Orientación y Aportes
  - ☐ Departamento de Recursos Humanos
  - ☐ Departamento de Abastecimiento
- ☐ Gerencia Zonal Lima Callao
- ☐ Gerencia de Formación Profesional para la Industria de la Const.
- ☐ Gerencia de Investigación y normalización para la vivienda y edif.
- ☐ *Escuela Superior Técnica*
  - ☐ Área de Administración y Finanzas
  - ☐ Biblioteca
  - ☐ Área de Servicios y Registros Académicos
  - ☐ Área de Coordinación Académica
  - ☐ Área de Promoción e Imagen
- ☐ Oficina de Planificación y Presupuesto
- ☐ Oficina de Secretaria General
  - ☐ Relaciones Públicas

Tipo de problema:

- ☐ Redes
- ☐ Hardware
- ☐ Software Base
- ☐ Soporte
- ☐ Soporte Office
- ☐ Aplicaciones
  - ☐ SAIS
  - ☐ APORTES
  - ☐ SISTEMA EDUCATIVO
  - Otros ☐ _____
- ☐ Web
  - Modulo:_____
- ☐

Descripción:

_____ Usuario	_____ Responsable del Área Usuaria(sello)

ANEXO N° 02
SGSI-FORM-37 BITÁCORA DE ACCESO AL DATA CENTER

Fecha	Nombres y Apellidos	Empresa	Autorizado Por	Motivo de Ingreso	Hora de Ingreso	Hora de Salida	Firma

ANEXO N° 03
ACUERDO DE CONFIDENCIALIDAD

Conste por el presente documento que yo: ……, identificado(a) con D.N.I. Nº ……, domiciliado(a) en …….. que como consecuencia de la labor que desempeño en el Servicio Nacional de Capacitación para la Industria de la Construcción (SENCICO) y teniendo acceso a información, cuyo término significa cualquier información escrita, gráfica, oral, electromagnética o de cualquier otro tipo, de propiedad del SENCICO, me comprometo indefinidamente a:

1. Mantener la información en estricta reserva y confidencialidad, no divulgarla acto alguno de la información a otra persona, ya sea natural o jurídica.
2. No usar la información directa o indirectamente en beneficio propio o de terceros, excepto para cumplir a cabalidad mis funciones relacionadas al puesto que desempeño.
3. No revelar total o parcialmente a otra persona, ya sea natural o jurídica, la información obtenida como consecuencia directa o indirecta de las conversaciones y/o de la prestación de servicios en el puesto que desempeño.
4. No utilizar unidades removibles y/o computadoras portátiles, sin autorización escrita del SENCICO y en caso contrario, sólo para los fines que me fueron autorizados.
5. No enviar a otra persona, ya sea natural o jurídica, archivos que contengan información de propiedad del SENCICO a través de correo electrónico, servicios en la nube u otros medios a los que tenga acceso, sin la autorización respectiva.

Asimismo, dejo constancia que tengo conocimiento de lo establecido por la normatividad referida a “Seguridad de la información”, la cual me comprometo a cumplir.

Así, en caso de incumplimiento de lo estipulado en el presente documento, me someto a las sanciones contenidas en las normas generales e instrumentos internos vigentes del SENCICO aplicables a mi modalidad contractual.

Para constancia de lo anterior, suscrito entre este acuerdo de confidencialidad en pleno uso de mis facultades, a los …… días de…… del año…….

……..
FIRMA

DNI N° ……

Huella dactilar

ANEXO N° 04
INSTRUCTIVO DE GESTIÓN DE USUARIOS

1. OBJETIVO

Definir las actividades para la creación, modificación y baja de cuentas de usuarios, así como las necesarias para la gestión de los accesos a los sistemas, servicios de red y/o recursos de tecnologías de información usando autenticación.

2. ALCANCE

El instructivo inicia con la solicitud de acceso requerida por el área solicitante y finaliza con la recepción de cierre de solicitud.

3. REFERENCIAS

- **Instructivo anterior:** N/A.
- **Instructivo posterior:** N/A.

4. BASE LEGAL

- Directiva GG/OAF/INF N° 003-2013 "Normas para el Uso del Servicio de Telefonía Fija"
- Resolución Ministerial N° 004-2016-PCM, del 08 de enero del 2016: Aprueban el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información, Requisitos. 2ª Edición” en todas las entidades integrantes del Sistema Nacional de Informática.

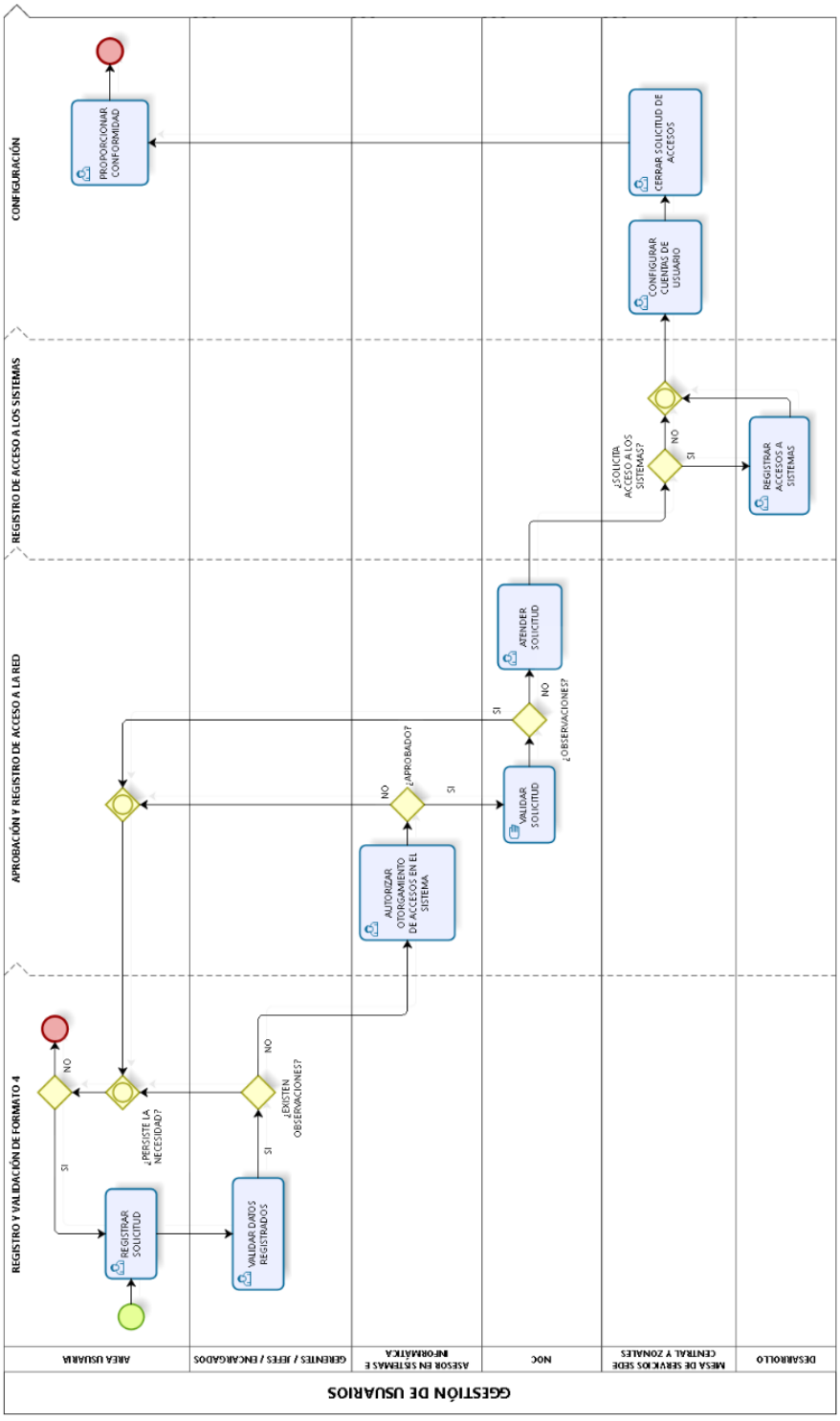
5. DEFINICIONES

- **Acceso:** Ingreso exitoso a un sistema, servicio de red o recurso de tecnología de la información a través de autenticación.
- **Aplicativo:** programa informático que permite al usuario realizar una o diversas tareas.
- **Autenticación:** Es el acto o proceso de confirmar que algo (o alguien) es quien dice ser (credenciales de usuario) a acceder a un sistema, servicio de red o recurso de tecnología de la información.
- **Código FAC:** credencial numérica que permite al usuario autenticarse en el sistema de telefonía para efectuar llamadas salientes externas.
- **Correo electrónico:** servicio que permite el intercambio de mensajes electrónicos a través de servidores de correo.
- **Credenciales de usuario:** son datos como el nombre de usuario y contraseña que se envían a un sistema para su autenticación.
- **Servicios de red:** servicios de tecnología de la información que se ofrecen a través de la red LAN/WAN, por ejemplo: carpetas de usuario en un servidor, Internet, correo electrónico, mensajería instantánea, etc.

6. SIGLAS / ABREVIATURAS

- **MSTI:** Mesa de Servicio de Tecnologías de Información.
- **NOC:** Network Operations Center (Centro de Control de la Red).

7. FLUJOGRAMA



8. DESCRIPCIÓN DEL INSTRUCTIVO

N°	Actividad	Descripción	Responsable	Registro	Tiempo
1	Registrar solicitud	Registra la solicitud de acceso a los servicios de red, correo electrónico, Internet, código FAC, aplicativos, etc. Para el registro de la solicitud, el usuario deberá tener en cuenta el Anexo 2 de este instructivo. (Para acceder y registrar la solicitud se debe ingresar a: http://ultron.sanborja.sencico.gob.pe/prd/waFormato4/ (Intranet). Una vez elaborada la solicitud el sistema enviará un mensaje de correo electrónico al Gerente o Jefe inmediato para su autorización.	Unidad Orgánica	Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES	5 - 10 min
2	Validar Datos Registrados	Valida los datos registrados en la solicitud. De estar conforme autoriza los accesos requeridos por el colaborador en la solicitud de acuerdo a las funciones que este desempeñará; luego el sistema envía un mensaje de correo al Asesor en Sistemas e Informática. En caso contrario se deniega la solicitud y se anota el motivo. El sistema envía un mensaje de correo al usuario comunicando la denegación de la solicitud. Si persiste la necesidad de acceso, el usuario modifica la solicitud (Continúa en la actividad N° 01). De lo contrario finaliza la solicitud. El responsable de la Unidad Orgánica deberá tener en cuenta el Anexo A de este instructivo	Responsable de la Unidad Orgánica	Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES	15 min

N°	Actividad	Descripción	Responsable	Registro	Tiempo
3	Autorizar otorgamiento de accesos en el Sistema	Autoriza que el personal de Informática brinde los accesos solicitados. En caso no se autorice los accesos, se comunica al área usuaria y de persistir la necesidad continúa en la actividad N° 01. Cuando se autoriza la solicitud el sistema envía un mensaje de correo al usuario de Informática con el rol de Administrador de red.	Asesor en Sistemas e Informática	Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES	10 min – 30 min
4	Validar solicitud	Valida los datos registrados en la solicitud. Si no está correcta, observa la solicitud y el sistema le envía un mensaje de correo al usuario notificándole las observaciones para que haga las modificaciones necesarias de persistir la necesidad de acceso. Se regresa a la actividad 1.	Administrador de red encargado de atender requerimientos de usuario	Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES	10 min – 20 min
5	Atender solicitud	Atiende la solicitud: Para la Sede Central y Zonales las credenciales de las cuentas de usuario creadas se envían por correo electrónico a la MSTI (red y correo electrónico). El código FAC se envía también a través del Sistema de Tarificación a la cuenta de correo del usuario (sede central). Actualización de archivos y sistemas necesarios documentando los accesos.	Administrador de red encargado de atender requerimientos de usuario	Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES	10 min – 20 min
6	Registrar Accesos a Sistemas	Registran acceso a los sistemas, para lo cual: Valida que los accesos a los sistemas tengan el visto bueno del propietario, según el Anexo 1: “Lineamientos Para La Solicitud De Accesos”.	Desarrollador	Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES	10 min – 20 min

N°	Actividad	Descripción	Responsable	Registro	Tiempo
		Crea, modifica o deshabilita los accesos a los sistemas. El sistema notifica la creación de los accesos a MSTI para que verifique que ya se configuraron los accesos a los sistemas. Notifica al usuario sobre los accesos brindados.			
7	Configurar cuentas de usuario	Configura los accesos a los aplicativos y servicios solicitados en el sitio del usuario. Si el usuario es de una Gerencia Zonal o Unidad Operativa coordina con el personal de soporte técnico de la zonal para que realice esta configuración. Si no se dispone de una persona de soporte técnico, accede a la computadora del usuario remotamente para efectuar las configuraciones necesarias.	Especialista de la MSTI encargado de atender los requerimientos de usuario en el sitio o en forma remota		20 min
8	Cerrar solicitud de accesos	Verifica que la solicitud ya fue atendida en su totalidad. Cierra la solicitud de accesos en el sistema y notifica al usuario de la culminación del servicio para la emisión de la conformidad.	Especialista de la MSTI encargado de gestionar los requerimientos de usuario a través del sistema	Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES	5min
9	Proporcionar conformidad	Proporciona la conformidad del servicio, completando la encuesta de satisfacción del servicio. Si el usuario no da la conformidad dentro de los primeros cinco días de atendida la solicitud, el sistema cambiará automáticamente el estado de la solicitud a “CONFORME”.	Usuario designado de la Unidad Orgánica	Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES	10 min
Tiempo empleado en el instructivo					**100 min – 160 min**

9. PUNTOS DE CONTROL

- N/A.

10. ANEXOS

- Anexo A: Lineamientos para la solicitud de accesos.
- Anexo B: Manual de Usuario del Sistema “Solicitud de Accesos a Servicios de Red y Aplicaciones”.

ANEXO A
LINEAMIENTOS PARA LA SOLICITUD DE ACCESOS

1. El Gerente o Jefe inmediato deberá designar a uno o más usuarios que estará(n) autorizado(s) para registrar las solicitudes de acceso en el aplicativo "Solicitud de Accesos a Servicios de Red y Aplicaciones" al cual se accede desde la intranet del SENCICO o desde el url:

   http://ultron.sanborja.sencico.gob.pe/prd/waFormato4/

2. Los usuarios para quienes se puede brindar acceso a los servicios de red del SENCICO son los colaboradores que trabajan en el SENCICO en la modalidad 728, 276, CAS o practicante y los contratados por locación de servicios (OS).

3. Antes de registrar la solicitud, el usuario debe verificar lo siguiente:
   a) Que la persona para quien se solicita los accesos ya debe haber sido dado de alta en los sistemas por el Departamento de Recursos Humanos.
   b) Que se haya generado la Orden de Servicios por parte del Departamento de Abastecimiento.
   c) Que la Orden de Servicios emitida especifique las armadas.

4. Los servicios que se atienden con el sistema son:
   a) Usuario Nuevo, para el caso del usuario que recién ingresa al SENCICO o que ya cesó, o terminó su contrato y está reingresando nuevamente.
   b) Cambio de Perfil, que ocurre cuando un usuario con contrato vigente, requiere modificación de sus accesos o acceso adicional.
      Los casos son los siguientes:
      - Cambio de modalidad de contratación de Orden de Servicios (OS) a Contrato Administrativo de Servicios (CAS) en la misma dependencia.
      - Cambio de dependencia y sigue trabajando en la modalidad de OS.
      - Solicita código FAC (sólo para 728, CAS y Practicantes)
      - Solicitan acceso a aplicativos.
      - Solicita cuenta de correo adicional. Las cuentas de correo electrónico asignados al personal contratado por OS son genéricas y están bajo la responsabilidad del gerente/jefe inmediato.
      - Para el caso de un usuario que requiere modificación de sus accesos o acceso adicional (aplicativos, carpetas, código FAC).
   c) Renovación de accesos, Para el caso del usuario con nueva fecha de vencimiento de contrato. En este caso se dan los mismos accesos que tenía antes de la fecha de término.
   d) Revocación de accesos (usuario sigue trabajando en la institución en otra dependencia). Lo solicita la dependencia en la que estuvo trabajando el usuario antes del cambio.
   e) Bajas de usuario (cese, término de contrato y término de orden de servicio).

5. Los códigos FAC solamente se asignan a los empleados: DL 728, 276, CAS y practicantes. Los códigos FAC usados por los terceros contratados por Orden de Servicio, son solicitados a nombre del gerente/jefe inmediato quien es responsable de su buen uso.

6. Los códigos FAC para las Gerencias Zonales Arequipa, Piura, Cusco, Trujillo y Chiclayo son creados por el personal técnico de la respectiva dependencia zonal. No se deben solicitar a través del Aplicativo: SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES.

7. El responsable de la Unidad Orgánica es responsable por los accesos que solicite para sus empleados y terceros autorizados, autorizando los que necesite para que cumpla sus funciones.

8. El responsable de la Unidad Orgánica deberá prever que el registro de la solicitud de accesos se haga con la debida anticipación para que sus empleados y terceros autorizados no paralice sus labores por falta de acceso a los servicios de red.

9. Del acceso a los sistemas
   Para acceder a un sistema debe tener el visto bueno del propietario del sistema. Para ello el usuario deberá registrar la justificación por la cual está solicitando el acceso. Si el propietario del sistema es el responsable de la unidad orgánica no requiere el visto bueno.
   El sistema enviará un mensaje de correo para que el propietario del sistema dé su visto bueno.

10. Del propietario de los sistemas
    El propietario del sistema da el visto bueno para que un usuario de otra unidad orgánica tenga acceso al sistema. Esto ocurre, por ejemplo, cuando un usuario del Departamento de Abastecimiento solicita acceso al sistema de Personal o de Control de Aportes.

    Los propietarios de los sistemas son los siguientes:
    a) Sistema de Logística y Abastecimiento, Jefe del Departamento de Abastecimiento.
    b) Sistema de Almacén, Jefe del Departamento de Abastecimiento.
    c) Sistema CAS, Jefe del Departamento de Recursos Humanos.
    d) Sistema de Patrimonio, Jefe del Departamento de Abastecimiento.
    e) Sistema de Contabilidad, Jefe del Departamento de Contabilidad. De uso exclusivo de la sede central.
    f) Sistema de Personal, Jefe del Departamento de Recursos Humanos.
    g) Sistema de Presupuesto, Gerente de la Oficina de Planificación y Presupuesto.
    h) Sistema de Tesorería, Jefe del Departamento de Tesorería.
    i) Sistema de Usuarios, Gerente de la Oficina de Planificación y Presupuesto.
    j) Sistema SIS, Gerente de la Oficina de Formación Profesional.
    k) Sistema de Control de Aportes, Jefe del Departamento de Orientación y Control de Aportes.
    l) Sistema SITRADOC, Secretaría General.
    m) Sistema Panel de Gestión, Secretaría General.
    n) Sistema SISCAR, Jefe del Departamento de Abastecimiento.
    o) Sistema SIGESCAP, Jefe del Departamento de Recursos Humanos.
    p) Sistema SIGESPER, Jefe del Departamento de Recursos Humanos. Para los empleados: DL 728, 276, CAS y practicantes sin necesidad de solicitarlo.

    No requieren del visto bueno del propietario del sistema los siguientes sistemas:
    - Sistema SITRADOC. Todos los empleados: DL. 728, 276 y CAS, Orden de Servicio y practicante utilizan cuentas genéricas si efectúan actividades secretariales.
    - Usuarios.

11. De las carpetas de usuario en los servidores

    Para acceso a las carpetas de usuario existen tres tipos de acceso:
    - Lectura (RX).
    - Lectura y Escritura (RXW).
    - Administrativo (ADM) para gerentes/jefes.

    Las carpetas de usuario son de uso exclusivo de la dependencia que solicitó su creación.

ANEXO B

MANUAL DE USUARIO DEL SISTEMA "SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES"

1. Inicio:

La dirección del sistema es: http://app.sencico.gob.pe/prd/waFormato4 . Para el ingreso al sistema se utiliza la misma cuenta de la red.

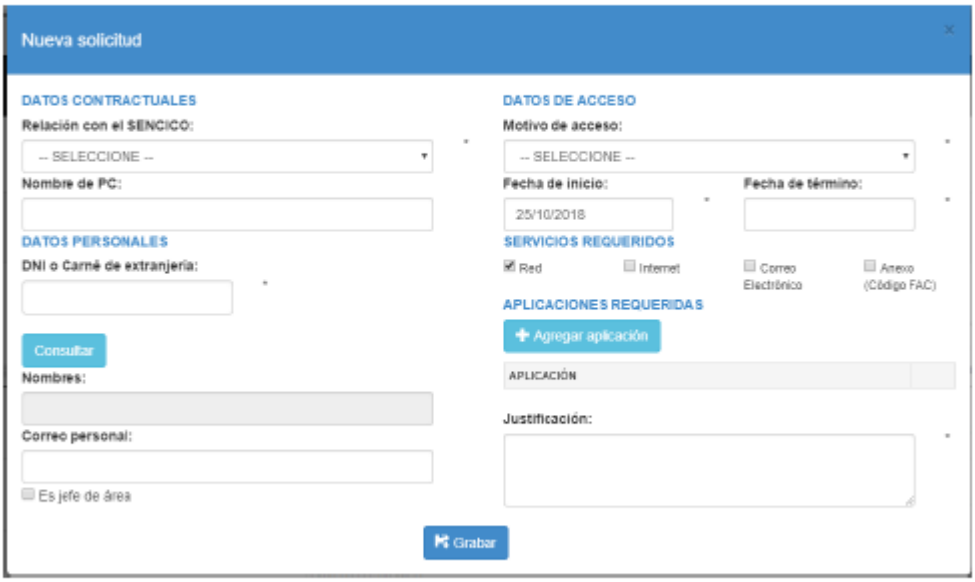
Presenta los siguientes roles:

- Usuario: Registra la solicitud de acceso.
- Jefe: Aprueba la solicitud generada por el usuario.
- Jefe Informática: Aprueba la solicitud aprobada por el jefe del área.
- Administrador de red: Crea las credenciales de red, correo y código FAC.
- Mesa de servicios: Crea los accesos a los sistemas.
- Usuario Informática: Realiza mantenimiento de accesos y roles.

2. Generación de solicitud:

SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

Para generar nueva solicitud, dar click en "Nueva Solicitud".



Llenamos todos los campos. Para ubicar el nombre del solicitante digitamos su número del documento de identidad y damos click en consultar.

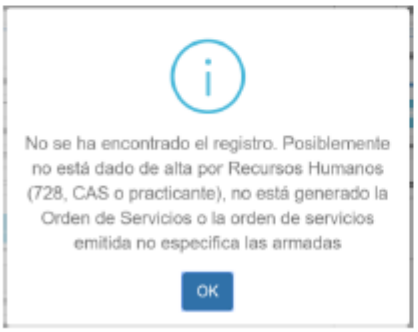
Nota: Para consultar los datos del solicitante, primero debe estar seleccionado la "Relación con el SENCICO". Si es personal contratado por locación de servicios, pedirá como datos documento de identidad y número de RUC.

En Relación con el SENCICO tenemos D.L. 728, D.L. 276, CAS, Practicante y O/S.

En motivos de acceso tenemos Usuario Nuevo, Renovación de acceso y Cambio de perfil.

- **Usuario nuevo:** Son aquellos usuarios que recién ingresan a la institución o los que regresan a la institución después de su cese de su vínculo laboral.
- **Renovación de acceso:** Son aquellos usuarios que se les han renovado su vínculo laboral con la institución.
- **Cambio de perfil:** son aquellos usuarios que, por necesidad de sus labores, soliciten accesos a otros aplicativos o carpetas de la red.

Si al consultar los datos personales aparece el siguiente mensaje:



SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

Se tendrá que esperar de uno a tres días en caso que sea D.L. 728, CAS o practicante, si es orden de servicios, depende de la demora del Departamento de Abastecimiento.

Si el solicitante va a ser jefe de área, activar la opción "Es jefe de área".

En aplicaciones requeridas debe agregar las aplicaciones que desea tener acceso. Si no requiere de acceso a ningún sistema o carpeta de la red (ejemplo carpeta SIAF) se deja en blanco.

Para agregar los accesos a los sistemas, click en el botón "Agregar aplicación". Nos muestra la siguiente ventana:

Selecciona el aplicativo y el rol y para confirmar dar click en "Agregar".

Para grabar la solicitud, damos click en "Grabar". El estado de la solicitud será "Pendiente".

3. Aprobar acceso por parte del jefe del área:

Esta opción es para los jefes de área.

Para atender, dar click en  .

SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

Para autorizar, dar click en "Autorizar". Al autorizar, el estado de la solicitud pasará a "Aprobado por la dependencia".

Para denegar dar click en "Denegar", aparecerá el siguiente cuadro:

Describe el motivo y para confirmar dar click en "Aceptar".

4. Autorización por parte del jefe de Informática:

Esta opción es para el titular del Departamento de Informática. Autoriza que el personal de Informática brinde los accesos solicitados.

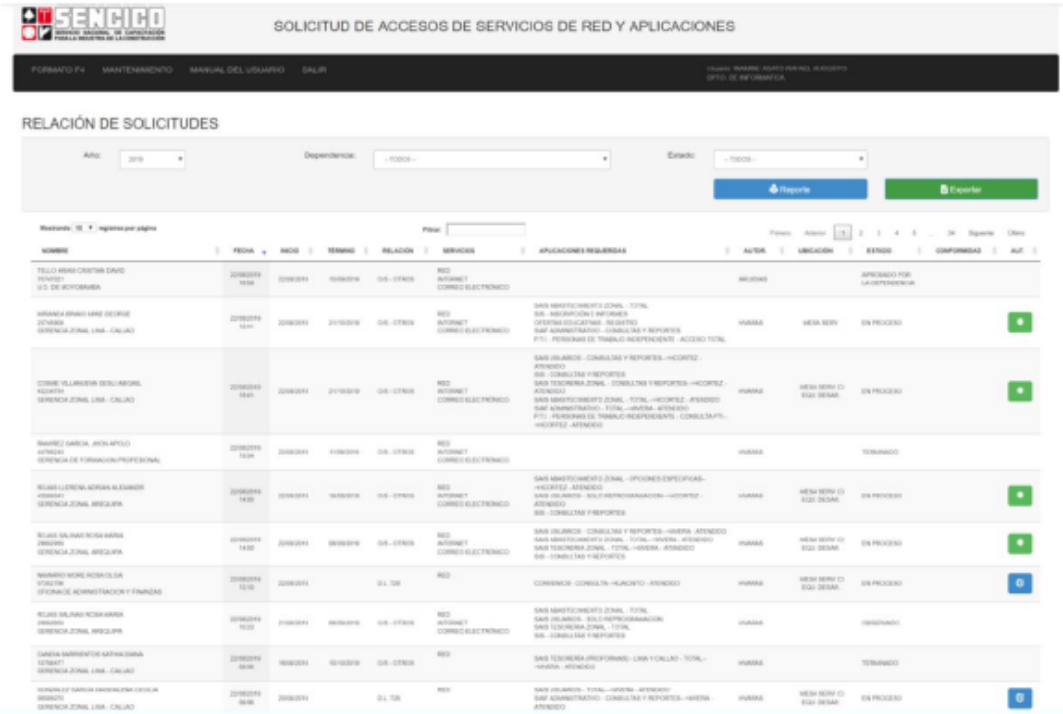
SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

Aquí llegaran las solicitudes que son previamente aprobadas por el jefe de área. También llegarán solicitudes registradas por cada área que tienen activada la opción "Es jefe de área" y las solicitudes propias del Departamento de Informática. Para atender es lo mismo que el de jefe de área.

Al aprobar, el estado de la solicitud pasará "En Proceso" y llegará primero al usuario de Informática con rol "Administrador de red".

5. Atención de solicitudes por el administrador de red:

El usuario con rol de administrador de red puede enviar credenciales de red, correo y código FAC; puede validar renovación y atender accesos a carpetas y/o sistemas; puede realizar mantenimiento a la tabla de accesos.



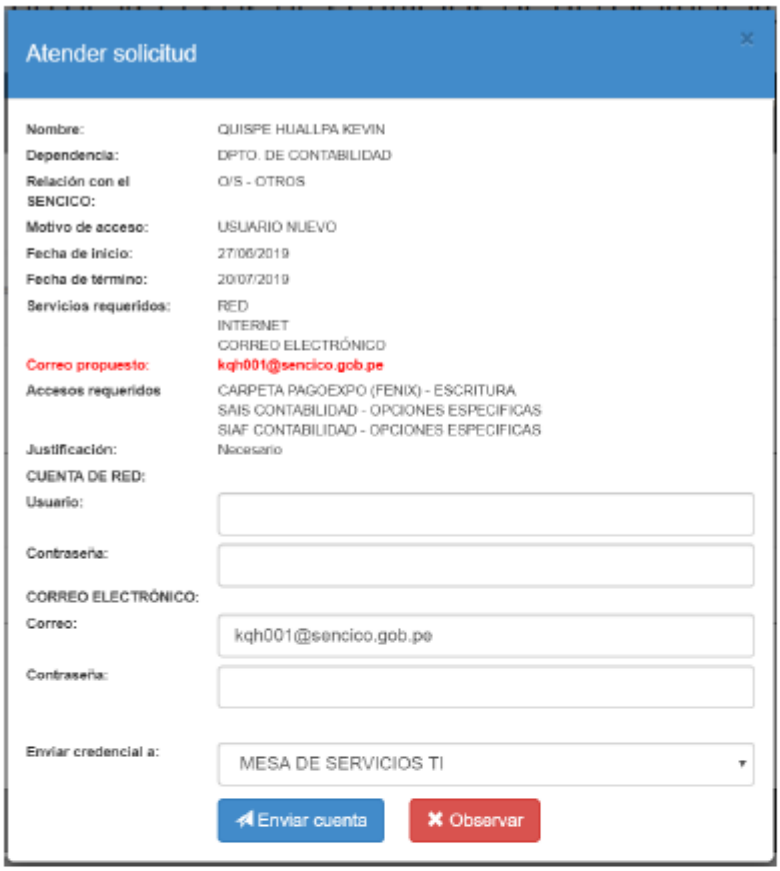
Atender envío de credenciales de red, correo electrónico y código FAC.

Validar acceso o cambio de perfil.

Atender accesos.

Al atender envío de credenciales aparecerá el siguiente cuadro:

SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

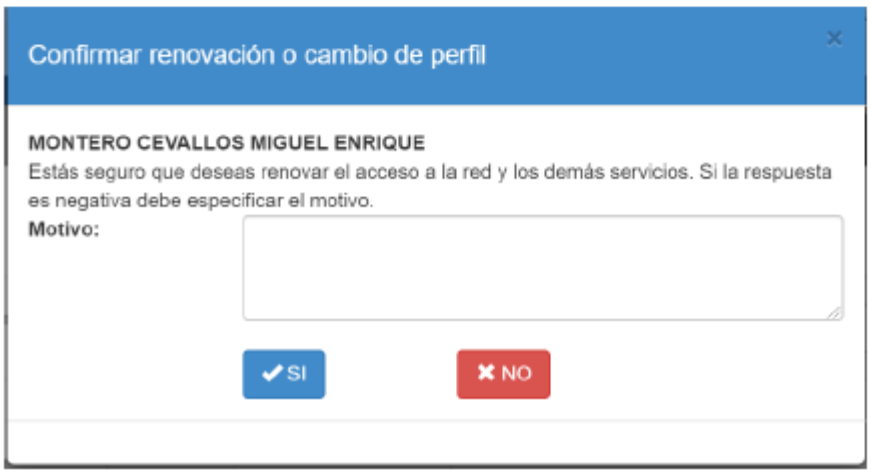


Llena los datos, en "Enviar credencial a:" si es usuario de sede central enviar a Mesa de Servicios TI, en caso de zonal, cambiar al correo que configuró en la solicitud.

Para confirmar, dar click en "Enviar cuenta", si tiene observación, dar click en "Observar".

Después de atender, el botón cambia a  para que pueda ser atendido por la mesa de servicios.

Para renovación mostrará la siguiente ventana:

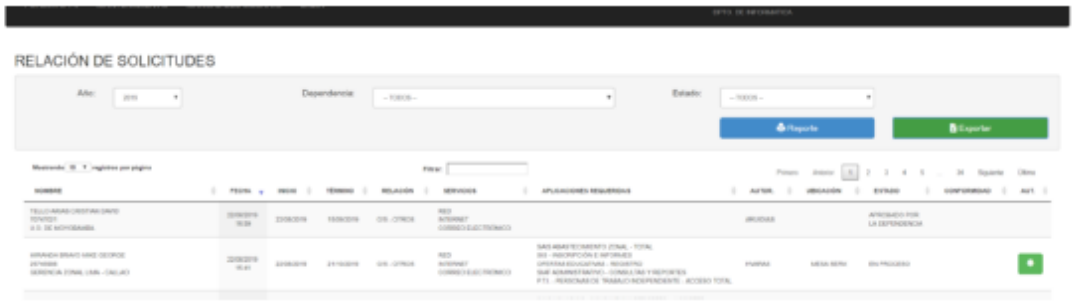


SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

Para cambio de perfil mostrará la siguiente ventana:

Antes de dar click en el botón "NO" debe especificar el motivo.

6. Atención de solicitudes por Mesa de Servicios TI:

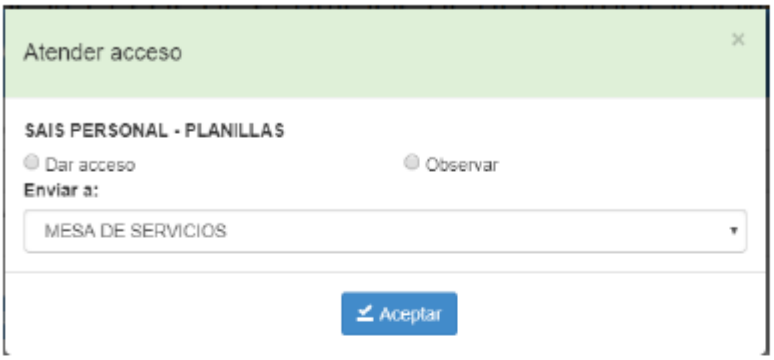


Las solicitudes que tienen el botón  pueden ser atendidas por la Mesa de Servicios TI.
Al dar click nos mostrará el siguiente cuadro:

El botón  es para delegar a los usuarios con rol de "Usuario Informática".

SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

Para dar el acceso, dar click en  . Nos mostrará el siguiente cuadro:



Tenemos las dos opciones: "Dar acceso" y "Observar".

Si marcamos "Dar acceso":

Llenamos los datos, en enviar a seleccionamos Mesa de Servicios si es usuario de la Sede Central, y si es zonal, cambiamos al correo personal que registró en el formato. Para terminar, damos click en "Aceptar".

Nota: si la cuenta de acceso es la misma que la cuenta de red, detallamos en "Sugerencia"

7. Atención de solicitudes por parte del equipo de desarrollo:

Esta opción es para los usuarios con rol de "Usuario Informática". Nos mostrará las solicitudes que la Mesa de Servicios les habilita. El procedimiento de atención es el mismo que el de Mesa de Servicios.

8. Finalizar atención de la solicitud:

Esta opción se encuentra disponible para los usuarios que tiene como rol de Mesa de Servicios. Para finalizar dar click en el botón  de la solicitud que va a dar por finalizado.

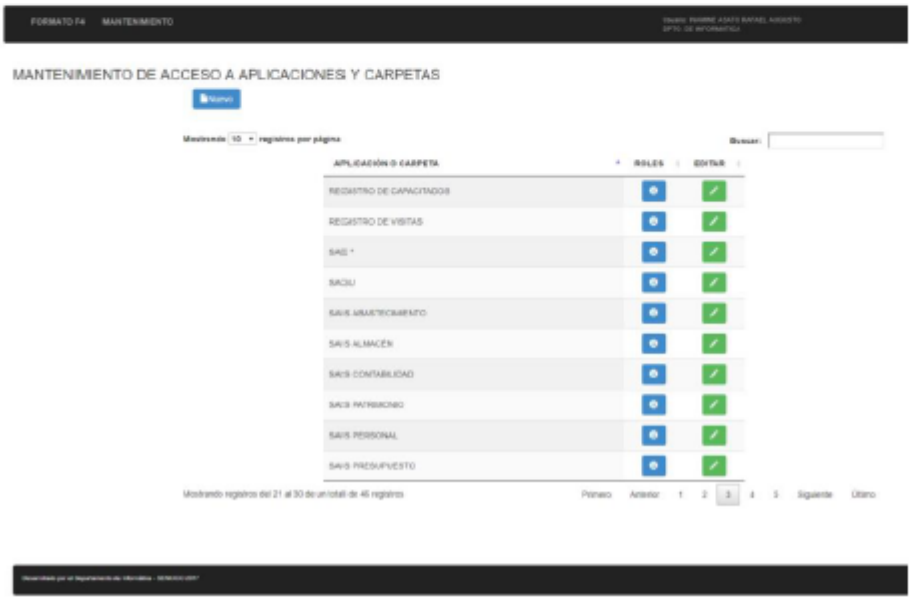
SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

Al dar click en el mencionado botón, nos aparecerá el siguiente cuadro de diálogo:

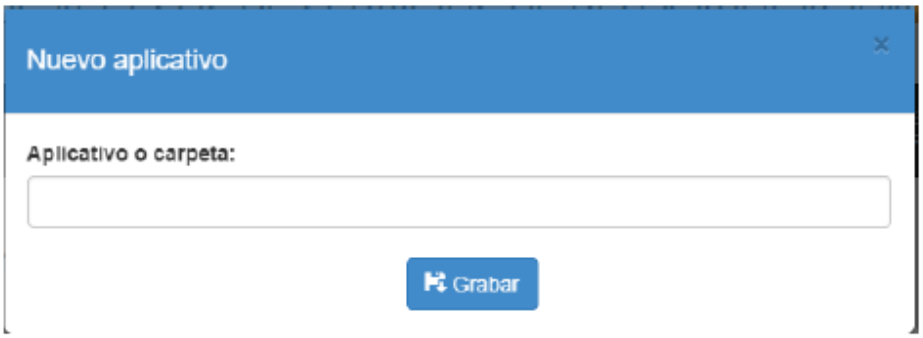
Para confirmar, dar en el botón "SI" y automáticamente pasará al estado de "terminado".

9. Mantenimiento de los Accesos:

Esta opción está disponible para los usuarios con roles de "Administrador de Red", "Mesa de Servicios" y "Usuario Informática". Para acceder, en el menú click en "Mantenimiento".



Para agregar nuevo ítem, dar click en "Nuevo". Nos mostrará la siguiente ventana:



Agregamos el nombre y para grabar damos click en "Grabar".

Para Modificar damos click en .

Para agregar los roles, damos click en . Nos muestra el siguiente cuadro:

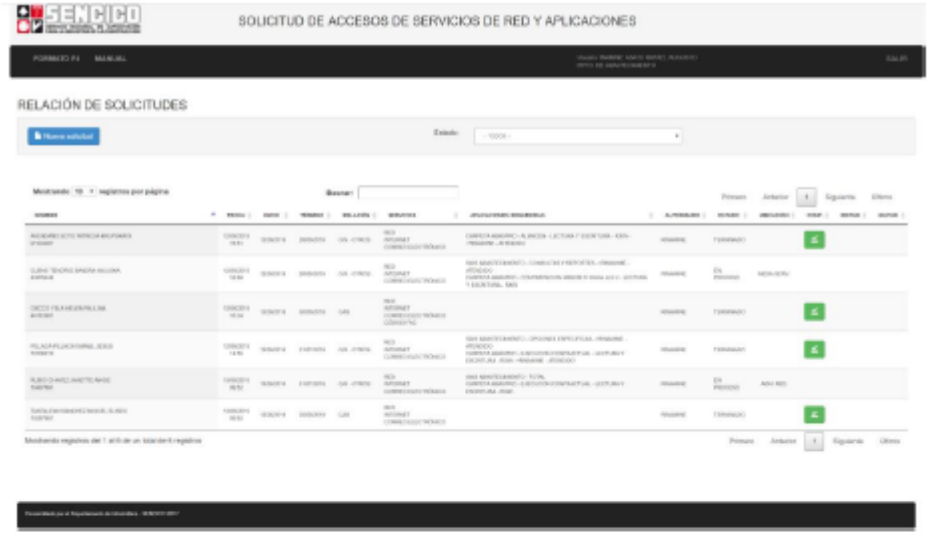
Para agregar el rol, damos click en "Nuevo".

Escribimos el rol y para terminar damos click en Grabar.

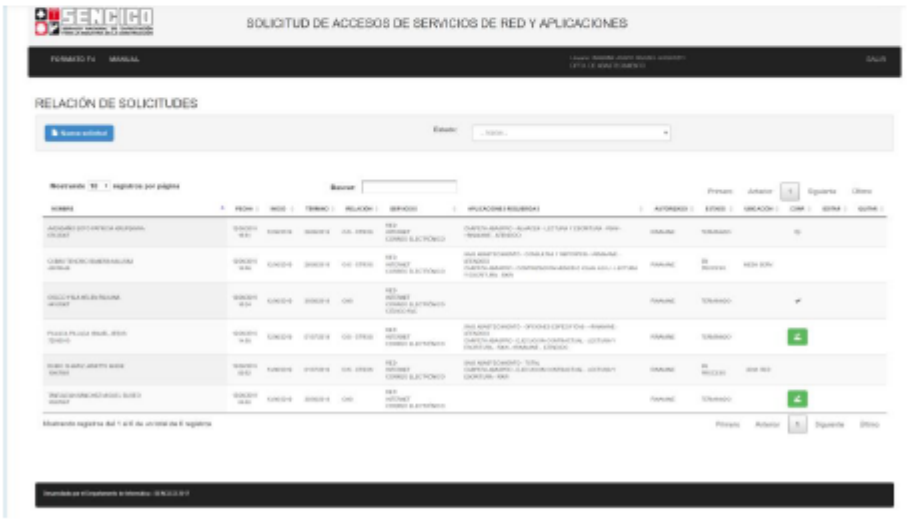
10. Conformidad de la atención de la solicitud:

Esta opción se encuentra en el rol de usuario, para dar la conformidad, dar click en el botón .

SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES



Nos mostrará el siguiente mensaje:



Si está conforme, cambia a , los no conforme nos muestra el .

Nota: Si no da conformidad dentro de los cinco primeros días de la atención de la solicitud, el sistema cambiará automáticamente al estado de "CONFORME".

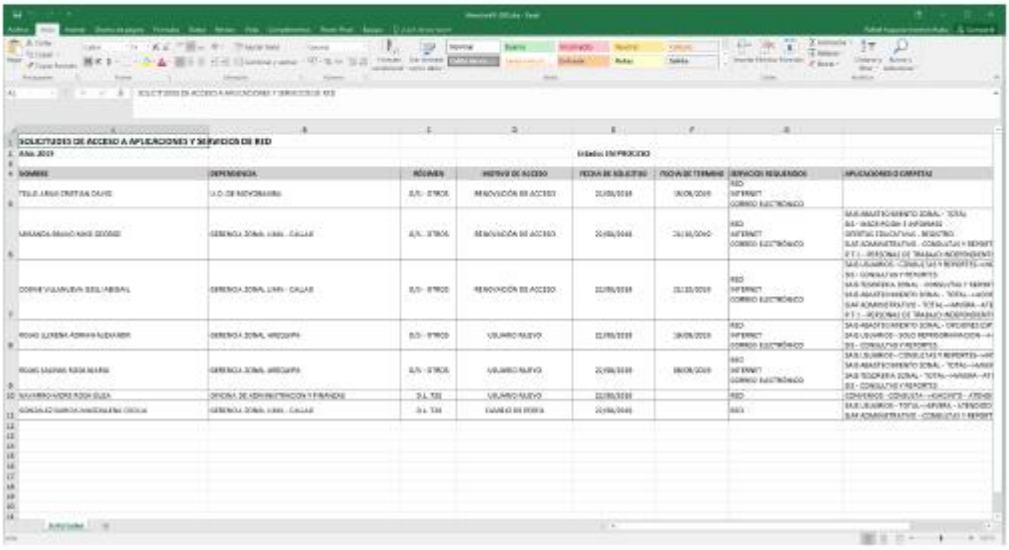
SOLICITUD DE ACCESOS A SERVICIOS DE RED Y APLICACIONES

11. Imprimir lista de solicitudes:

Esta opción se encuentra disponible para los que tienen rol de "Administrador de red", "Mesa de servicios" y "Usuario Informática". Para imprimir el reporte, dar click en el botón "Reporte". Nos mostrará el reporte en formato PDF en una ventana aparte.

12. Exportar a Excel lista de solicitudes:

Esta opción se encuentra disponible para los que tienen rol de "Administrador de red", "Mesa de servicios" y "Usuario Informática". Para exportar a excel, dar click en "Exportar".



ANEXO N° 05

INSTRUCTIVO DE SEGURIDAD Y CORRECTO USO DE LAS INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN

1. OBJETIVO

El objetivo de este instructivo es poder controlar el acceso al Data Center, con la finalidad de evitar el acceso de los empleados del SENCICO y terceros no autorizado al mismo.

2. ALCANCE

El instructivo inicia con la solicitud de autorización de ingreso y finaliza con el registro de salida de la data center y ocurrencias.

3. REFERENCIAS

- **Instructivo anterior:** N/A.
- **Instructivo posterior:** N/A.

4. BASE LEGAL

Resolución Ministerial N° 004-2016-PCM, del 08 de enero del 2016: Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información, Requisitos. 2ª Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

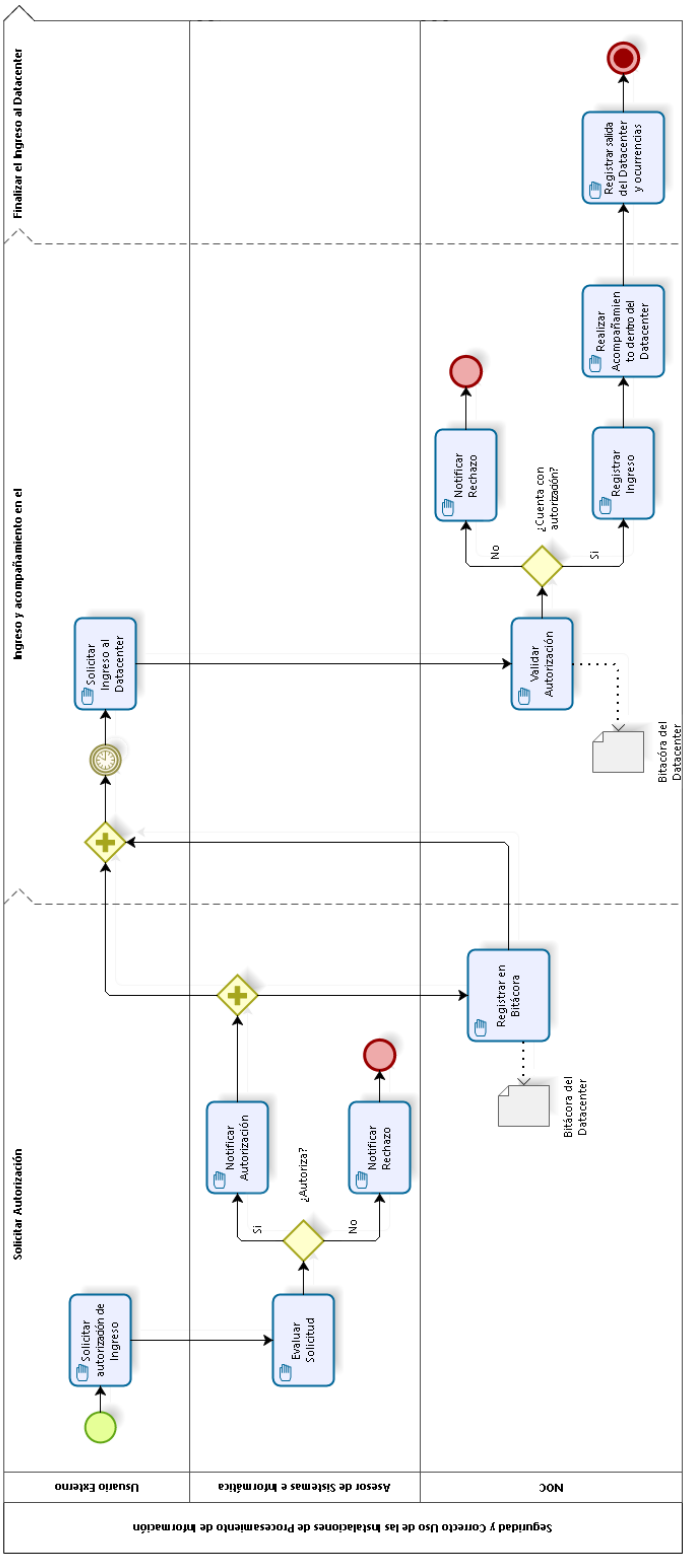
5. DEFINICIONES

- **Tecnología de Información (TI):** Se refiere al hardware y software operados por la Institución o por un tercero sin tener en cuenta la tecnología utilizada.
- **Bitácora de Acceso al Data Center:** Documento físico en el cual se registra todos los ingresos y salidas de personal interno o externo al Data Center.

6. SIGLAS / ABREVIATURAS

- **NOC:** Network Operations Center (Centro de Control de la Red).

7. FLUJOGRAMA



8. DESCRIPCIÓN DEL INSTRUCTIVO

N°	Actividad	Descripción	Responsable	Registro	Tiempo
1	Solicitar autorización de Ingreso	Solicita autorización de ingreso mediante correo, Carta y/o Oficio, informe y/o memorando (de considerar necesario contar con registro fotográfico, se deberá justificar).	Usuario Externo	Correo, *0105+Carta y/o Oficio, Informe y/o Memorando	10 min una vez recepcionada por Asesor en Sistemas e Informática
2	Evaluar solicitud	Evalúa solicitud de acceso, para lo cual lo aprueba o desestima. En el caso de autorizar continúa en la actividad N°04, caso contrario continúa en la actividad N° 03.	Asesor en Sistemas e Informática		15 min
3	Notificar rechazo	Notifica rechazo al área usuaria.	Asesor en Sistemas e Informática		5 min
4	Notificar autorización	Notifica autorización al usuario visitante y al personal del NOC. Continúa de manera paralela en la actividad N°05 y N°06.	Asesor en Sistemas e Informática		-----
5	Registrar en Bitácora	Registra en la Bitácora del Datacenter los siguientes datos mínimos: - Nombres completos. - DNI. - Fecha de Ingreso. - Justificación del ingreso. - Hora de Ingreso y salida.	Responsable del NOC	Bitácora	5 min
6	Solicitar ingreso al Datacenter	Solicita ingreso al Datacenter.	Usuario Externo		5 min
7	Validar autorización	Valida autorización en la Bitácora. En caso se cuente con autorización, continúa en la actividad N° 09, caso contrario continúa en la actividad N° 08.	Responsable del NOC	Bitácora	5 min
8	Notifica rechazo	Notifica rechazo al usuario externo.	Responsable del NOC		

N°	Actividad	Descripción	Responsable	Registro	Tiempo
9	Registrar ingreso		Responsable del NOC	Bitácora	5 min
10	Realizar acompañamiento dentro del Datacenter	Realiza acompañamiento a la visita durante su estadía en el Datacenter.	Personal del NOC		--
11	Registrar salida del Datacenter y ocurrencias	Registra la salida del Datacenter y las ocurrencias que pudieron darse durante la visita.	Personal del NOC		5 min
Tiempo empleado en el instructivo					**55 min**

9. PUNTOS DE CONTROL

- N/A.

10. ANEXOS

- N/A.

ANEXO N° 06

INSTRUCTIVO DE RESPALDO Y RESTAURACIÓN

1. OBJETIVO

Gestionar el respaldo y recuperación de la información, definir las pautas generales para proteger y salvaguardar la integridad y disponibilidad de la información del SENCICO, para recuperarla en situaciones de desastre e indisponibilidad de los servicios de tecnología de información.

2. ALCANCE

El instructivo inicia con la solicitud de respaldo de información realizado por la unidad orgánica solicitante y finaliza con la conformidad de servicio brindada.

3. REFERENCIAS

- **Instructivo anterior:** N/A.
- **Instructivo posterior:** N/A.

4. BASE LEGAL

Resolución Ministerial N° 004-2016-PCM, del 08 de enero del 2016: Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información, Requisitos. 2ª Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

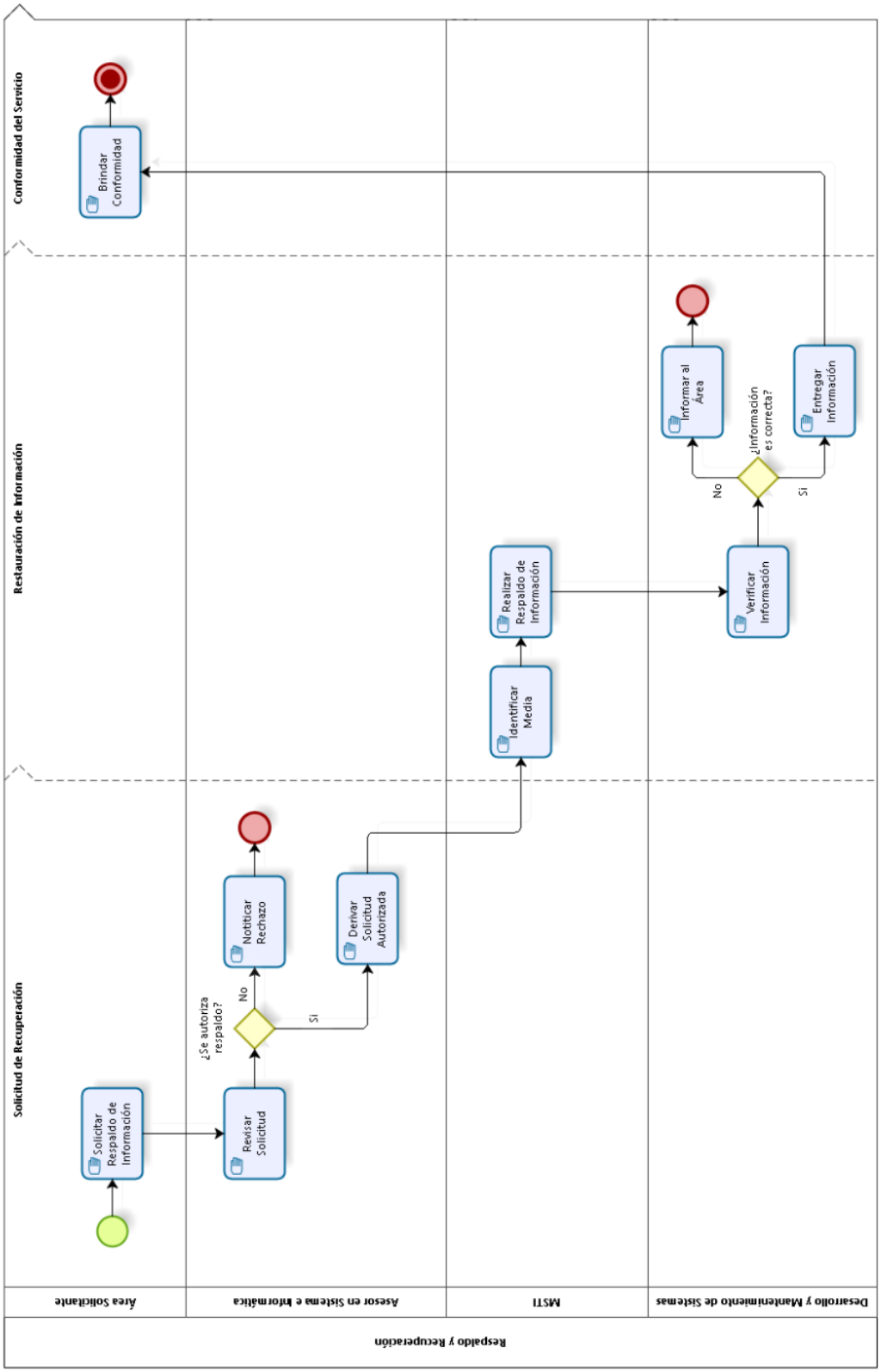
5. DEFINICIONES

- **Medios de Almacenamiento (media):** Cualquier dispositivo capaz de recibir información y retenerla durante un periodo de tiempo, permitiendo su recuperación y empleo cuando sea necesario. Pueden ser de tipo magnético (cintas, USBs, discos duros, discos compactos CD, DVD, entre otros).
- **Lector/Grabador de Medios Respaldo/Librería:** Dispositivo que se utiliza para grabar la data y recuperarla con los medios de almacenamiento.
- **Respaldo Total:** Archivo de respaldo que contiene un almacenamiento completo de la información. Este respaldo se puede hacer sin necesidad de algún archivo respaldo base.
- **Usuario:** Empleados del SENCICO a nivel nacional y terceros autorizados que tienen asignado un equipo informático y hace uso de él.
- **Información a Respaldar:** Toda la información que se genere para los procesos de negocio.

6. SIGLAS / ABREVIATURAS

- N/A.

7. FLUJOGRAMA



8. DESCRIPCIÓN DEL INSTRUCTIVO

Nº	Actividad	Descripción	Responsable	Registro	Tiempo
1	Solicitar respaldo de Información	Solicita respaldo de información por correo electrónico al Asesor en Sistemas e Informática indicando la fuente de la información que se desea respaldar.	Usuario de Unidad Orgánica	Formato F4	10 min
2	Autorizar respaldo	Autoriza respaldo o lo desestima. En el caso de autorizar se continúa en la actividad N° 04, caso contrario continúa en la actividad N° 03.	Asesor en Sistemas e Informática		15 min
3	Notificar rechazo	Notifica al área usuaria la razón del rechazo.	Asesor en Sistemas e Informática		10 min – 30 min
4	Identificar media	Identifica la media donde se va a respaldar la información la cual es proporcionada por el usuario.	MSTI	SYSAID	2 min
5	Realizar respaldo de Información	Realiza respaldo de información a una media entregada por el usuario.	MSTI	SYSAID	5 min - 10 min
6	Verificar información	Verifica información respaldada a fin que el proceso se haya llevado correctamente. Si es correcta continúa en la actividad N° 09, caso contrario continúa en la actividad N° 08.	Especialista en Infraestructura de redes y comunicaciones		10 min – 20 min
7	Informar al área	Informa al área usuaria que el respaldo no fue exitoso con las razones técnicas.	Especialista en Desarrollo y Mantenimiento de Sistemas		10 min – 20 min
8	Entregar información	Entrega la información al área usuaria.	MSTI		20 min
9	Dar conformidad	El usuario emite la conformidad respectiva luego de recibido el servicio.	Usuario de Unidad Orgánica		10 min
Tiempo empleado en el instructivo					**122 min – 167 min**

9. PUNTOS DE CONTROL

- N/A.

10. ANEXOS

- N/A.

ANEXO N° 07

INSTRUCTIVO DE TRASLADO DE CINTAS DE RESPALDO

1. OBJETIVO

El instructivo tiene como objetivo gestionar el traslado de la cinta de respaldo, para un resguardo externo.

2. ALCANCE

El presente procedimiento inicia con la programación de traslado de cintas de respaldo y finaliza con la emisión de un informe técnico detallando las cintas entregadas para resguardo externo.

3. REFERENCIAS

- **Instructivo anterior:** N/A.
- **Instructivo posterior:** N/A.

4. BASE LEGAL

- Resolución Ministerial N° 004-2016-PCM, del 08 de enero del 2016: Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información, Requisitos. 2ª Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Jefatural N° 386-2002-INEI – Aprueba Directiva N° 016-2002-INEI/DTNP – Normas Técnicas para el almacenamiento y respaldo de la información procesada por las entidades de la administración pública.

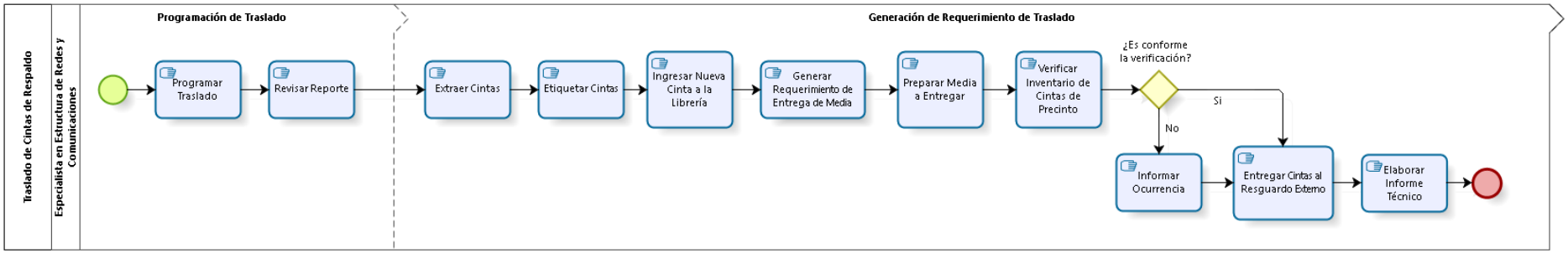
5. DEFINICIONES

- **Medios de Almacenamiento (media):** Cualquier dispositivo capaz de recibir información y retenerla durante un periodo de tiempo, permitiendo su recuperación y empleo cuando sea necesario. Pueden ser de tipo magnético (cintas, USBs, discos duros, discos compactos CD, DVD, entre otros).
- **Ambiente de Prueba:** Describe la ubicación en la que se ven previamente los cambios en un software y son ajustados antes de su publicación final (producción).

6. SIGLAS / ABREVIATURAS

- **BD:** Base de Datos.

7. FLUJOGRAMA



8. DESCRIPCIÓN DEL INSTRUCTIVO

N°	Actividad	Descripción	Responsable	Registro	Tiempo
1	Programar traslado	Programa traslado de cintas en un cronograma.	Especialista en Infraestructura de Redes y Comunicaciones		10 min – 30 min
2	Revisar reporte	Revisa reporte de resumen de cintas a fin de identificar qué cinta debe extraerse para su traslado.	Especialista en Infraestructura de Redes y Comunicaciones		5 min – 10 min
3	Extraer Cintas	Extrae cintas de respaldo, para lo cual se ejecutan los siguientes comandos en la librería de Backup: • *run ret_offsite LABEL* para los backups de archivos • *run ret_cinta LABEL* para los backups de la BD y del tipo archive Se verifica que la cinta se encuentre en la lista: *query libvol*, para luego retirarla físicamente del Slot I/O Station.	Especialista en Infraestructura de Redes y Comunicaciones		10 min – 30 min
4	Etiquetar Cintas	Etiqueta cintas mediante la colocación de una etiqueta de código de barra emitida por el fabricante de las cintas. Una vez que la cinta está llena se extrae de la Librería de Backup y se rotula, de acuerdo a la codificación siguiente: - Una para la base de datos y copias de respaldo tipo archive: BLTO_DB_D/ALTO_FIL_M/BLTO_FIL_D, ETIQUETA DE CÓDIGOS DE BARRAS y FECHA DE RETIRO de la cinta. - Una para archivos, tablas DBF: CLTO_CPY_D/CLTO_CPY_M, ETIQUETA DE CÓDIGOS DE BARRAS y FECHA DE RETIRO de la cinta.	Especialista en Infraestructura de Redes y Comunicaciones		10 min - 30 min

N°	Actividad	Descripción	Responsable	Registro	Tiempo
5	Ingresar nueva Cinta a la Librería	Ingresa nueva cinta a la librería, para lo cual, previamente coloca la etiqueta de código de barras. Posteriormente: Ingresar cinta scratch a la librería en un slot libre del magazine y ejecuta los siguientes comandos: • *run ing_scratch (inventario de cinta en blanco)* • *query libvol (para verificar que la nueva cinta figura en la librería)*	Especialista en Infraestructura de Redes y Comunicaciones		10 min - 30 min
6	Generar el requerimiento de Entrega de Media	Genera el requerimiento de entrega de media, para lo cual ingresa al site www.securesync.com, los siguientes datos requeridos: - Usuario. - Contraseña. - Fecha del servicio. - ID del contenedor. Con los datos anteriores, Iron Mountain genera el reporte SolicitarEntregarMedios, con un Request ID que identifica el pedido.	Especialista en Infraestructura de Redes y Comunicaciones		5 min – 10 min
7	Preparar Media a entregar	Prepara media a entregar, para lo cual elabora un reporte de entrega de cintas denominado “Registro de Cintas entregadas al resguardo externo mes en curso AAAA.xls”. Posteriormente, fotografía las cintas a entregar al resguardo externo.	Especialista en Infraestructura de Redes y Comunicaciones		10 min – 20 min
8	Verificar inventario de cintas y precinto	Verifica inventario de cintas y precinto, por lo cual, el día del servicio, se entregan las cintas al personal de Iron Mountain. El personal de Iron Mountain registra el inventario de las cintas entregadas en el Request Detail Report, el cual es visado y firmado por el personal del NOC encargado de entregar las cintas. El personal de Iron Mountain rompe el precinto de seguridad el cual es entregado a especialista en Infraestructura de Redes y	Especialista en Infraestructura de Redes y Comunicaciones		5 minutos

N°	Actividad	Descripción	Responsable	Registro	Tiempo
		Comunicaciones, encargado de entregar las cintas, para la verificación. En la verificación, el Especialista en Infraestructura de Redes y Comunicaciones valida que el precinto entregado es el mismo con el que se cerró el contenedor en la entrega anterior; de estar conforme pasa a la actividad 10, de no estar conforme pasa a la actividad 9.			
9	Informar ocurrencia	Informa ocurrencia al Asesor en Sistemas e Informática a fin que tome las acciones correspondientes.	Especialista en Infraestructura de Redes y Comunicaciones		5 minutos
10	Entregar Cintas al resguardo externo	Entrega cintas al resguardo externo, para lo cual se ingresan las cintas al contenedor asignado y solicitado con el Request ID. El personal de Iron Mountain procede con el cerrado de contenedor con un nuevo precinto el cual es fotografiado por el especialista de Infraestructura de Redes y Comunicaciones Posteriormente, ingresa el código asignado por Iron Mountain en el scanner de códigos y una vez validado el código se escanea el contenedor y se cierra la actividad.	Especialista en Infraestructura de Redes y Comunicaciones		10 min – 20 min
11	Elaborar Informe interno	Elabora informe interno el cual contiene los detalles de las cintas entregadas al resguardo externo y al cual se adjuntan: - Registro de Cintas entregadas al resguardo externo mes en curso AAAA.xls. - Reporte “SolicitarEntregarMedios”. - Formato “Request Detail Report”. - Fotografías de cintas y contenedor.	Especialista en Infraestructura de Redes y Comunicaciones		10 min – 20 min
Tiempo empleado en el instructivo					**90 min – 200 min**

9. PUNTOS DE CONTROL

- N/A.

10. ANEXOS

- N/A.

ANEXO N° 08

INSTRUCTIVO DE RECUPERACIÓN DE CINTAS DE RESPALDO

1. OBJETIVO

El instructivo tiene como objetivo restaurar la información de las cintas de respaldo, de acuerdo a las necesidades de la Institución.

2. ALCANCE

El presente procedimiento inicia con la solicitud de recuperación de información por parte de la unidad orgánica y finaliza con la conformidad brindada en la atención de la solicitud.

3. REFERENCIAS

- **Instructivo anterior:** N/A.
- **Instructivo posterior:** N/A.

4. BASE LEGAL

- Resolución Ministerial N° 004-2016-PCM, del 08 de enero del 2016: Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información, Requisitos. 2° Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

5. DEFINICIONES

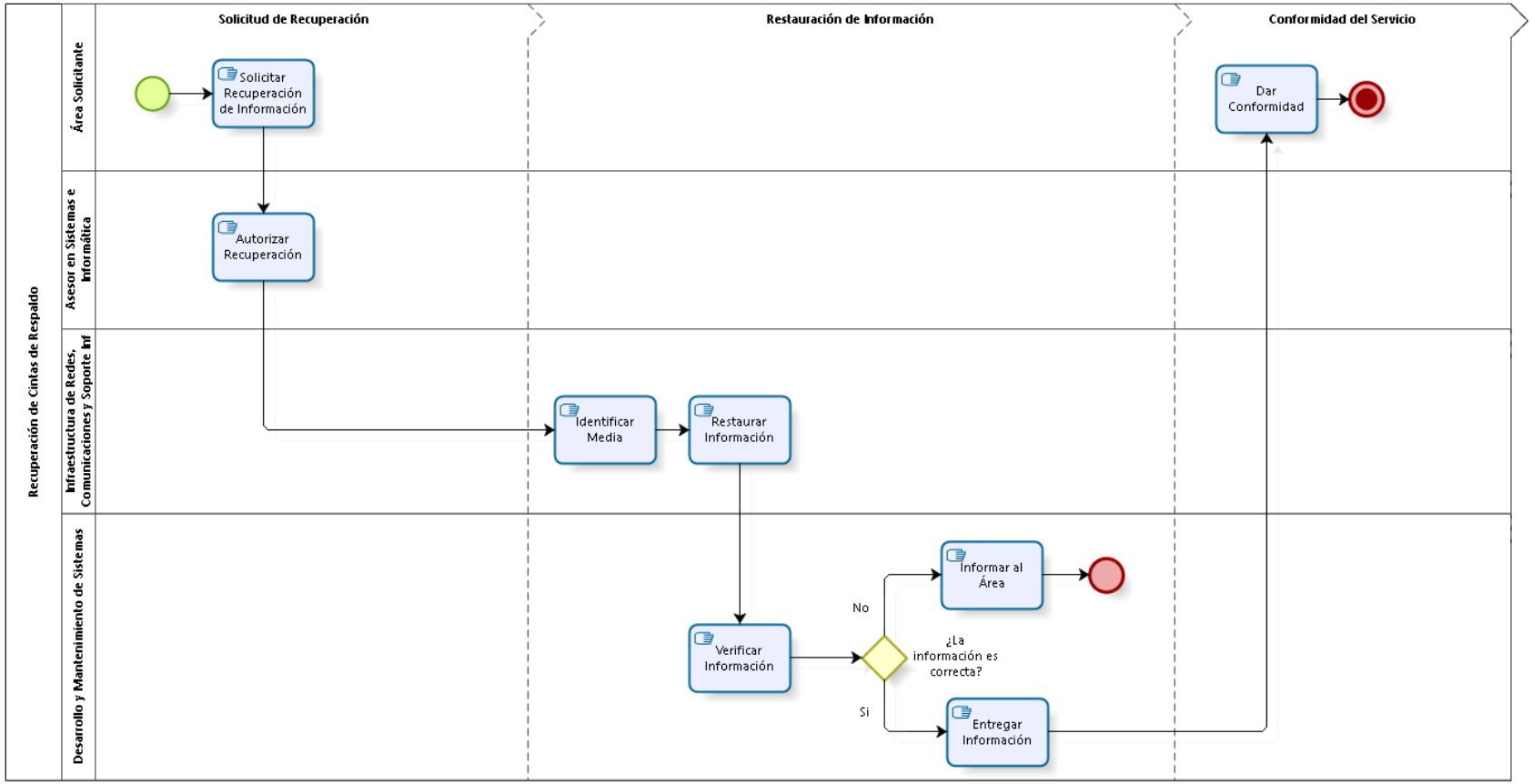
- **Medios de Almacenamiento (media):** Cualquier dispositivo capaz de recibir información y retenerla durante un periodo de tiempo, permitiendo su recuperación y empleo cuando sea necesario. Pueden ser de tipo magnético (cintas, USBs, discos duros, discos compactos CD, DVD, entre otros).

- **Ambiente de Prueba:** Describe la ubicación en la que se ven previamente los cambios en un software y son ajustados antes de su publicación final (producción).

6. SIGLAS / ABREVIATURAS

- N/A.

7. FLUJOGRAMA



8. DESCRIPCIÓN DEL INSTRUCTIVO

N°	Actividad	Descripción	Responsable	Registro	Tiempo
1	Solicitar recuperación de información	Solicita recuperación de información al Departamento de Informática, a través de correo electrónico o memorando al Asesor en Sistemas e Informática.	Usuario de Unidad Orgánica		10 min – 1 hr
2	Autorizar recuperación	Autoriza recuperación y deriva el requerimiento a la unidad correspondiente de Informática (Desarrollo y Mantenimiento de Sistemas o Infraestructura de Redes y Comunicaciones).	Asesor en Sistemas e Informática		1 hr
3	Identificar Media	Identifica media en la cual se encuentra ubicada la información requerida.	Especialista en Infraestructura de Redes y Comunicaciones		30 min – 1 hr
4	Restaurar Información	Restaura información a través del uso de un software o utilitario que restaura la información de la referida media a la cual se le indica la ubicación de destino de la información.	Especialista en Infraestructura de Redes y Comunicaciones		1 hr – 1 día
5	Verificar Información	Verifica información a través de pruebas realizadas por el especialista encargado del sistema que utiliza referida información, de no ser útil la información restaurada se continua en el punto 6, y para el caso de contar con la información requerida se continua en el punto 7.	Especialista en Desarrollo de Sistemas		30 min – 1 hr
6	Informar al área	Informa al área que la información no se recuperó correctamente.	Asesor en Sistemas e Informática		5 min - 10 min
7	Entregar Información	Entrega información requerida al área solicitante, en la media proporcionada o por medio de un sistema en un ambiente de prueba.	Especialista en Desarrollo de Sistemas		10 min – 1 hr

N°	Actividad	Descripción	Responsable	Registro	Tiempo
8	Dar conformidad	Da conformidad del servicio recibido.	Usuario		30 min – 1hr
Tiempo empleado en el instructivo					**235 min - 2 días**

9. PUNTOS DE CONTROL

- N/A.

10. ANEXOS

- N/A.