SENCICO
SERVICIO NACIONAL DE CAPACITACIÓN PARA LA INDUSTRIA DE LA CONSTRUCCIÓN

DIRECTIVA DE SEGURIDAD INFORMATICA DE LA RED DEL SENCICO

RESOLUCIÓN Nº 168-2024-02.00

Departamento de Informática

AGOSTO

2024

FIRMA DIGITAL
Firmado digitalmente por:
VARAS GRAUS Roger Hector
FAU 20131377810 soft
Motivo: Firmado
Digitalmente
Fecha: 28/08/2024 17:42:07-0500

Firmado digitalmente por
GUERRERO SILVA SOLIS Luis
Martin FAU 20131377810 soft
Motivo: Doy V° B°
Fecha: 28.08.2024 17:59:41 -05:00

<table>
<tr><td rowspan="4">SENCICO</td><td colspan="2">DIRECTIVA</td><td colspan="2">DI/PE/OAF/INF/ 02-2024</td></tr>
<tr><td colspan="4">TITULO: SEGURIDAD INFORMATICA DE LA RED DEL SENCICO</td></tr>
<tr><td>Aprobado por:</td><td>Presidencia Ejecutiva</td><td rowspan="2">Fecha de Aprobación:</td><td rowspan="2"></td></tr>
<tr><td>Propuesto por:</td><td>Departamento de Informática</td></tr>
<tr><td></td><td>Deja sin Efecto:</td><td>DI/PE/OAF-INF/N° 002-2020</td><td>Fecha de Publicación:</td><td></td></tr>
</table>

1. OBJETIVO

Establecer las disposiciones 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 preservar la confidencialidad, integridad y disponibilidad de los activos digitales.

2. ALCANCE

La presente Directiva es de aplicación para todos los servidores del SENCICO a nivel nacional y contratistas que acceden a los activos digitales del SENCICO.

3. 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.

4. BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Ley N° 28716, Ley de Control Interno de las entidades del Estado.
- Decreto Supremo N° 030-2002-PCM, que aprueba el 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.
- Decreto Supremo Nº 029-2021-PCM que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- 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.
- NTP ISO/IEC 27007:2007 Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de sistemas de gestión de seguridad de la información.
- Decreto Supremo N° 050-2018-PCM. Decreto que establece la definición de Seguridad Digital de ámbito nacional
- Decreto de Urgencia N° 007-2020. Decreto de urgencia que aprueba el marco de confianza digital
- Resolución de Presidencia Ejecutiva N° 134-2018-02.00. Conformación del Comité de Gobierno Digital del SENCICO
- Resolución de Presidencia Ejecutiva N° 82-2021-02.00. Designación del Oficial de Seguridad Digital del SENCICO

5. DEFINICIONES

5.1. **Accesos**: Permisos específicos que se le otorga al colaborador o contratista autorizado a los activos digitales del SENCICO.

5.2. **Acceso remoto:** Acceso a una red o un equipo de forma remota a través de una conexión a Internet.

5.3. **Actualizaciones de software:** Nuevas versiones de un software existente que incluyen modificaciones para mejorar su rendimiento, corregir errores o agregar nuevas características. Las actualizaciones de software pueden ser pequeñas o grandes y pueden incluir mejoras en la seguridad, la estabilidad y la compatibilidad.

5.4. **AES (Advanced Encryption Standard):** Algoritmo de cifra basado en un secreto compartido (clave). Cifra el texto en bloques de 128 bits. Utiliza claves de 128, 192 o 256 bits.

5.5. **Ambiente de desarrollo:** Ambiente donde se desarrolla el sistema de información y se realizan las pruebas iniciales.

5.6. **Ambiente de producción:** Ambiente donde el sistema de información se ejecuta al cual se conectan los usuarios finales y donde se trabaja con los datos de la institución.

5.7. **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).

5.8. **Análisis de vulnerabilidades:** Proceso de identificación y evaluación de las vulnerabilidades presentes en los sistemas y redes, con el fin de tomar medidas de mitigación y corrección para evitar su explotación.

5.9. **AntiDDoS (Anti-Distributed Denial of Service):** El AntiDDoS es un conjunto de técnicas y soluciones diseñadas para proteger una infraestructura de red contra ataques de denegación de servicio distribuidos (DDoS).

5.10. **Autenticación:** Proceso mediante el cual se verifica la identidad de un usuario o dispositivo antes de permitir el acceso a los sistemas o recursos. Puede involucrar el uso de contraseñas, tarjetas inteligentes, biometría u otros métodos de verificación.

5.11. **Cambios de configuraciones:** Modificaciones realizadas en la configuración de los sistemas y ambientes de desarrollo, como cambios en permisos de acceso, privilegios u otras configuraciones relacionadas con la seguridad.

5.12. **Certificado digital:** Conjunto de datos que identifica inequívocamente una entidad, contiene la clave pública de la entidad y otra información, y es firmado digitalmente por una parte confiable confirmando de esta manera su identidad en Internet.

5.13. **Cifrado:** Que está escrito con letras, símbolos o números que solo pueden comprenderse si se dispone de la clave criptográfica necesaria para descifrarlos.

5.14. **Claves criptográficas:** Conjunto de datos utilizados en algoritmos criptográficos para cifrar y descifrar información, preservando su confidencialidad e integridad.

5.15. **Código malicioso:** Software diseñado para dañar, comprometer o acceder de manera no autorizada a los sistemas y datos. Incluye virus, gusanos, troyanos, ransomware, entre otros.

5.16. **Copias de respaldo:** Copias de seguridad de los datos y sistemas almacenados en un entorno seguro, realizadas regularmente para preservar la disponibilidad y recuperación de la información en caso de pérdida o daño.

5.17. **CRC (Cyclic Redundancy Check):** Código de detección de errores que se usa comúnmente en redes digitales y dispositivos de almacenamiento para detectar cambios en los datos sin procesar.

5.18. **Credenciales:** Información utilizada para autenticar la identidad de un usuario o dispositivo, como nombres de usuario, contraseñas, certificados digitales, entre otros.

5.19. **Criptografía asimétrica:** Método de cifrado en el cual se utilizan dos claves diferentes, una para cifrar y otra para descifrar. Se conoce como cifrado de clave pública.

5.20. **Criptografía simétrica:** Método de cifrado en el cual se utiliza la misma clave para cifrar y descifrar los datos. Se conoce como cifrado de clave privada.

5.21. **CSIRT:** Equipo de respuesta a incidentes de seguridad digital (Computer Security Incident Response Team). Es responsable de coordinar y gestionar la respuesta a los incidentes de seguridad digital.

5.22. **CVSS 3.0 (Common Vulnerability Scoring System 3.0):** Estándar abierto y neutro de la industria cuya finalidad es proporcionar unas métricas para la comunicación de las características, impacto y severidad de vulnerabilidades que afectan a elementos del entorno de seguridad de TI y ayudar a determinar tanto la urgencia como la priorización de las actividades de respuesta para la corrección de vulnerabilidades. CVSS consta de tres grupos de métricas: base, temporal y ambiental.

5.23. **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.

5.24. **Database Administrator (DBA):** Administrador de bases de datos encargado de gestionar y mantener las bases de datos del SENCICO.

5.25. **Directorio Activo:** Base de datos jerárquica que proporciona la capacidad de establecer un único inicio de sesión y un repositorio central de información para toda la infraestructura, lo que simplifica ampliamente la administración de usuarios y equipos, proporcionando además la obtención de un acceso mejorado a los recursos en red.

5.26. **Dispositivos Móviles:** Equipos portátiles como teléfonos móviles, tabletas y laptops de propiedad del SENCICO, utilizados por los colaboradores para acceder y procesar información.

5.27. **DLP (Data Loss Prevention):** Conjunto de técnicas y políticas destinadas a prevenir la pérdida o divulgación no autorizada de datos sensibles. Utilizando diversas tecnologías, como el monitoreo de contenido, el cifrado, la identificación de patrones y la gestión de derechos de información.

5.28. **DSA (Digital Signature Algorithm):** Algoritmo criptográfico asimétrico para una firma digital en forma de un par de números grandes. La firma se calcula utilizando reglas y parámetros tales que se pueda verificar la identidad del firmante y la integridad de los datos firmados.

5.29. **ECDSA (Elliptic Curve Digital Signature Algorithm):** Es una modificación del algoritmo DSA que emplea operaciones sobre puntos de curvas elípticas en lugar de las exponenciaciones que usa DSA (problema del logaritmo discreto). La principal ventaja de este esquema es que requiere números de tamaños menores para brindar la misma seguridad que DSA o RSA.

5.30. **Endpoint Detection and Response (EDR):** Tecnología que detecta y responde a amenazas en los dispositivos finales de una red, como computadoras y dispositivos móviles.

5.31. **Enmascaramiento dinámico:** Técnica de enmascaramiento en tiempo real que se utiliza para proteger datos confidenciales, como datos personales, limitando su exposición según el principio de mínimo privilegio. Esta práctica implica alterar dinámicamente los datos confidenciales existentes a medida que los usuarios acceden a ellos o los consultan, para mostrarles solo una versión enmascarada si es que no tienen los privilegios necesarios para ver los datos completos.

5.32. **Ente Rector del Sistema Nacional de Transformación Digital:** Secretaria de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros.

5.33. **Equipos de infraestructura de TI:** Componentes físicos que proporcionan el soporte necesario para el funcionamiento de los sistemas de información y las operaciones de TI en general. Ejemplos: servidores de aplicaciones, dispositivos de almacenamiento de datos, equipos de red, equipos de seguridad, equipos de cómputo, entre otros.

5.34. **Ethical Hacking:** Consiste en realizar pruebas y evaluaciones de seguridad en sistemas informáticos, redes o aplicaciones, con el fin de identificar vulnerabilidades y debilidades antes de que sean explotadas.

5.35. **Evaluación de riesgos:** Proceso de identificación, análisis y evaluación de los riesgos que pueden afectar la seguridad de la información y los sistemas de una organización. Permite determinar las medidas de control necesarias para mitigar los riesgos identificados.

5.36. **FIPS 140-2 (Security Requirements for Cryptographic Modules):** Esta norma define los requisitos de seguridad que debe cumplir un módulo criptográfico utilizado en un sistema de seguridad que protege información no clasificada dentro de los sistemas de TI. Algunos aspectos relacionados con las claves criptográficas incluyen: a) generación de claves criptográficas utilizando fuentes de entropía

adecuadas, b) requisitos para el almacenamiento seguro de claves, incluyendo protección contra accesos no autorizados, c) especifica medidas para el transporte seguro de claves entre módulos criptográficos y d) otros aspectos.

5.37. **Firewall:** Dispositivo de seguridad que controla el tráfico de red, permitiendo o bloqueando el acceso a los sistemas y recursos según las reglas establecidas.

5.38. **Firma digital:** Resultado de la trasformación criptográfica de los datos, que cuando es apropiadamente implementada, provee los siguientes servicios: 1) autenticación de origen, 2) integridad de datos y 3) no repudiación del firmante.

5.39. **FTPS (FTP over SSL):** Protocolo de transferencia de archivos que utiliza SSL para asegurar los comandos y los datos que se transfieren entre el cliente y el servidor.

5.40. **HMAC (Hash-Based Message Authentication Code):** Técnica de autenticación de mensajes que incluye una clave secreta. De esta forma se detecta la manipulación del contenido al tiempo que se chequea una clave de autenticación.

5.41. **HTTPS (Hypertext Transfer Protocol Over Secure Socket Layer):** Protocolo que proporciona autenticación y comunicación cifrada en el Internet diseñado para comunicaciones que dependen de la seguridad, tales como los inicios de sesión basados en la web.

5.42. **Identificador único:** Número o código exclusivo asignado a cada usuario o dispositivo para identificarlo de manera única en los sistemas.

5.43. **Incidente de seguridad digital:** Evento que compromete la seguridad de la información, como el acceso no autorizado, la pérdida de datos, el software malicioso, entre otros.

5.44. **Información no pública:** Información contemplada expresamente en las excepciones establecidas en el Texto Único Ordenado de la Ley de Transparencia y Acceso a la Información Pública, Ley N° 27806 (TUO de la Ley): información secreta, información reservada e información confidencial.

5.45. **IPS (Intrusion Prevention System):** Un IPS es una solución de seguridad digital que monitorea y analiza el tráfico de red en busca de comportamientos o patrones sospechosos que puedan indicar un intento de intrusión o ataque.

5.46. **IPSEC:** Colección de mecanismos de protección que extienden los paquetes IP para proporcionar servicios de control de acceso, integridad, autenticación de origen, detección y rechazo de duplicados y confidencialidad.

5.47. **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).

5.48. **MAC (Message Authentication Code):** Es una porción de información utilizada para autenticar un mensaje.

5.49. **Módulo de criptografía:** Conjunto de hardware, software y/o firmware que implementa funciones aprobadas de seguridad (incluyendo algoritmos de criptografía y generación de claves) y es contenido dentro de los límites de la criptografía.

5.50. **Network Operations Center (NOC):** Centro de operaciones de red encargado de supervisar y gestionar el funcionamiento de la infraestructura de red de una organización.

5.51. **NIST SP (National Institute of Standards and Technology Special Publications):** NIST ha publicado varias publicaciones especiales relacionadas con el manejo de claves criptográficas que incluyen los siguientes aspectos: a) orientación general sobre la gestión de claves criptográficas, incluyendo la generación, distribución, almacenamiento y destrucción de claves, b) pautas específicas para la generación segura de claves criptográficas, c) orientación para la transición segura entre algoritmos criptográficos y longitudes de clave y d) otros aspectos.

5.52. **NGFW (Next-Generation Firewall):** Un NGFW es un tipo de firewall que combina las funcionalidades de un firewall tradicional con capacidades avanzadas de seguridad. Además de controlar el tráfico de red y aplicar políticas de acceso.

5.53. **NTP (Network Time Protocol):** Es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos.

5.54. **On premises:** Infraestructura de TI que se encuentra dentro de las instalaciones físicas del SENCICO, en lugar de estar ubicada en servidores o recursos alojados en la nube.

5.55. **OWASP API Security Top 10:** Documento estándar de referencia que busca brindar valor a los desarrolladores de software y evaluadores de seguridad al resaltar los riesgos potenciales de las API inseguras e ilustrar cómo se pueden mitigar estos riesgos.

5.56. **OWASP Mobile Top 10:** Documento estándar de referencia para desarrolladores y seguridad de aplicaciones móviles que representa un amplio consenso sobre los riesgos de seguridad más críticos para las aplicaciones móviles.

5.57. **OWASP Top 10:** Documento estándar de referencia para los riesgos de seguridad de aplicaciones web más críticos. Adoptar OWASP Top 10 es quizás el primer paso más eficaz para cambiar su cultura de desarrollo de software centrada en producir código seguro.

5.58. **Paquetes de software:** Conjunto de programas informáticos predefinidos y preescritos, que están disponibles de manera licenciada y que están diseñados para realizar funciones específicas sin la necesidad de escribir software personalizado desde cero. La instalación y el soporte de estos paquetes de software suelen requerir la intervención de programadores profesionales que lo puedan personalizar, configurar y mantener.

5.59. **Parches de software:** Actualizaciones pequeñas que se centran en corregir errores específicos o solucionar problemas de seguridad, sin tener que actualizar todo el software. Por lo general, los parches se lanzan después de que se descubre un problema y se desarrolla una solución.

5.60. **PGP (Pretty Good Privacy):** Programa de seguridad para correo electrónico cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

5.61. **Plataforma Colaborativa:** Conjunto de herramientas, aplicaciones y servicios de TI, diseñados para mejorar la productividad, fomentar la comunicación efectiva, compartir la información en entornos de trabajo y permitir la colaboración en tiempo real entre el personal. Ejemplos: Microsoft Teams, SharePoint, OneDrive, entre otras.

5.62. **Programas de utilidad privilegiados:** Herramientas de software que se utilizan para llevar a cabo tareas administrativas, de mantenimiento y gestión de sistemas y redes, y generalmente requieren niveles superiores de autorización para ejecutarse debido a la naturaleza crítica de las operaciones que realizan. Ejemplos: herramientas de copias de seguridad y restauración, herramientas de administración de redes, herramientas de diagnóstico o configuración del sistema, herramientas de gestión de seguridad, herramientas de virtualización, herramientas de monitoreo de recursos, entre otros.

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

5.64. **Resiliencia:** Capacidad de un sistema o infraestructura para resistir y recuperarse rápidamente de interrupciones, fallas o desastres, manteniendo la continuidad de las operaciones críticas.

5.65. **RSA (Rivest, Shamir y Adelman):** Cifrado asimétrico que se basa en operaciones de potenciación en aritmética modular y su fortaleza radica en la dificultad de factorizar números extraordinariamente grandes. Es, con gran diferencia, la técnica asimétrica de uso más generalizado. Su longitud de clave (pública y privada) es variable, siendo valores usuales: 512, 1024, 2048 o 3072

bits. Frente a otras técnicas asimétricas presenta la ventaja de poderse emplear también en la firma digital.

5.66. **Sandboxing:** Es una técnica de seguridad que consiste en ejecutar aplicaciones, archivos o procesos en un entorno aislado y controlado, conocido como “sandbox”.

5.67. **Servicios de mensajería:** Servicios que permiten el intercambio de mensajes y comunicación entre colaboradores del SENCICO.

5.68. **Seguridad de la Información:** Conjunto de medidas y acciones destinadas a proteger la confidencialidad, integridad y disponibilidad de la información, así como los sistemas y recursos que la procesan, almacenan y transmiten.

5.69. **SFTP (SSH FTP):** Protocolo que transmite los datos de control y transferencia de manera encriptada y por un único canal utilizando el protocolo SSH.

5.70. **Sistemas de prevención de intrusiones (IPS/IDS):** Tecnologías que detectan y previenen el ingreso de tráfico malicioso e indeseado a la red, protegiéndola de ataques y asegurando su disponibilidad.

5.71. **S/MIME (Secure / Multipurpose Internet Mail Extensions):** Estándar para criptografía de clave pública y firmado de correo electrónico encapsulado en MIME.

5.72. **Soporte de sistemas:** Componentes que respaldan el funcionamiento de los sistemas de información. Ejemplos: servidores de aplicaciones, soluciones de almacenamiento de datos, redes, bases de datos, entre otros.

5.73. **Software:** Conjunto de instrucciones técnicamente denominadas programas, que realizan operaciones o tareas específicas. El software puede ser de los siguientes tipos: a) software de aplicación que ofrecen una funcionalidad específica para ayudar a los usuarios a realizar tareas determinadas (sistemas de información, aplicaciones, procesadores de texto, software de base de datos, navegadores, multimedia, etc.), b) software de sistema o software de base que facilita las operaciones entre el software de aplicación y los componentes de hardware presentes en los dispositivos (sistema operativo, controlador, firmware, utilitario, entre otros), y c) software de programación que permiten crear nuevos software.

5.74. **SSH (Secure Shell):** Nombre de un protocolo y del programa que lo implementa. Este protocolo sirve para acceder a máquinas remotas a través de una red, de forma similar a como se hace con "telnet" con la diferencia principal de que SSH usa técnicas de cifrado en el intercambio de información.

5.75. **SSL (Secure Sockets Layer):** Protocolo para navegadores web y servidores que permite la autenticación, encriptación y desencriptación de datos enviados a través de Internet.

5.76. **TLS (Transport Layer Security):** Es la versión mejorada del protocolo SSL, siendo más estable y seguro.

5.77. **Súper Usuario:** Usuario que posee los más altos privilegios en un determinado sistema o plataforma de TI.

5.78. **Trabajo a distancia:** Teletrabajo o trabajo remoto.

5.79. **Trabajo remoto**: Prestación de servicios subordinada con la presencia física del trabajador en su domicilio o lugar de aislamiento domiciliario, utilizando cualquier medio o mecanismo que posibilite realizar las labores fuera del SENCICO, siempre que la naturaleza de las labores lo permita.

5.80. **Uninterruptible Power Supply (UPS):** Dispositivo que proporciona energía eléctrica de respaldo en caso de interrupciones o fluctuaciones en el suministro eléctrico.

5.81. **Usuario:** Persona autorizada que utiliza los sistemas y recursos de información del SENCICO para llevar a cabo sus funciones y tareas asignadas.

5.82. **Vulnerabilidad:** Debilidad o fallo en un sistema o proceso que puede ser explotado por un atacante para comprometer la seguridad de la información. Puede ser causada por errores de configuración, falta de parches o diseño inseguro.

5.83. **VPN (Virtual Private Network):** Una técnica para conectar una red desde una ubicación remota usando el Internet como medio de red.

5.84. **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).

5.85. **Web Application Firewall (WAF):** Es un tipo de firewall cuya función es inspeccionar el tráfico entrante y saliente de las aplicaciones web, filtrando, vigilando y bloqueando el tráfico malicioso.

5.86. **WPA3 (Wi-Fi Protected Access 3):** Protocolo de seguridad para conexiones Wi-Fi diseñado para mejorar la seguridad en conexiones inalámbricas.

5.87. **Zero Trust (Confianza cero):** Enfoque de seguridad digital que asume que no se debe confiar por defecto en ningún usuario, dispositivo o sistema, tanto si están dentro o fuera de la red del SENCICO, verificando su identidad y autenticación.

6. ABREVIATURAS

- **CSIRT:** Equipo de respuesta a incidentes de seguridad digital (Computer Security Incident Response Team).

7. RESPONSABILIDADES

7.1. GERENTES Y/O JEFES DE LAS UNIDADES DE ORGANIZACIÓN

7.1.1. Involucrar y dar facilidades a su personal para el cumplimiento de sus deberes y obligaciones en materia de seguridad digital.

7.1.2. Asegurar el cumplimiento normativo en materia de seguridad digital.

7.1.3. Participar de manera eficaz en la gestión de los riesgos, eventos e incidentes de seguridad de digital.

7.1.4. Reportar todo incidente de seguridad digital que afecte los procesos y servicios que brinda la unidad de organización, de forma inmediata.

7.1.5. Gestionar la implementación de los controles de seguridad digital identificados en sus ámbitos de competencia, así como también coadyuvar en la gestión e incidentes de seguridad digital.

7.2. DEL DEPARTAMENTO DE INFORMÁTICA

7.2.1. Planificar, implementar, ejecutar y supervisar el uso y adopción de las tecnologías digitales como habilitantes de la implementación de la cadena de valor, priorizadas en el marco de los instrumentos de gestión del SENCICO, con el propósito de permitir alcanzar sus objetivos estratégicos, crear valor público y cumplir con lo establecido por el Comité de Gobierno Digital del SENCICO.

7.2.2. Diseñar los servicios digitales del SENCICO atendiendo las necesidades de disponibilidad, integridad y confidencialidad de la información que se captura, procesa y distribuye.

7.2.3. Coordinar la implementación y mantenimiento del SGSI en la entidad, atendiendo las normas en materia de seguridad digital, confianza digital y gobierno digital.

7.3. DE LOS COLABORADORES Y CONTRATISTAS

7.3.1. Cumplir con los deberes y obligaciones en materia de seguridad digital.

8. DISPOSICIONES GENERALES

8.1. El SENCICO cuenta con activos físicos y digitales, así como instalaciones asociadas que le permiten alcanzar sus objetivos estratégicos, los cuales son identificados y gestionados de acuerdo con su importancia, clasificación y los riesgos de seguridad de la información asociados.

8.2. Los colaboradores y contratistas deben involucrarse en la gestión y operación de la seguridad de la información en el SENCICO, de acuerdo con las responsabilidades definidas en la presente directiva.

8.3. El Departamento de Informática limita los accesos a los activos físicos y digitales, así como a las instalaciones asociadas, a los colaboradores, contratistas, procesos y equipos autorizados; y los gestiona previa evaluación de riesgos que considera la posibilidad de acceso no autorizado a actividades y transacciones legítimas en el SENCICO.

8.4. El Departamento de Informática ejecuta y mantiene los planes y procedimientos de recuperación de los servicios de TI en el SENCICO para asegurar la disponibilidad de sistemas de información, aplicaciones u otros activos afectados por incidentes de seguridad.

8.5. El Departamento de Informática establece contacto con diferentes grupos de interés (medios e investigadores especializados que envían actualizaciones, avisos de alertas, noticias o boletines de seguridad de la Información). Estos contactos están registrados a través del Anexo N° 01: Matriz de Contacto con Grupos de Interés.

8.6. El Departamento de Informática realiza el mantenimiento de los componentes de los sistemas de información, aplicaciones, servicios de red e infraestructura de TI de acuerdo con la normativa interna de seguridad de la información.

8.7. El Departamento de Informática gestiona la adquisición de soluciones de seguridad digital para preservar la integridad y confidencialidad de la información, así como la disponibilidad de los sistemas de información, aplicaciones y otros activos, de acuerdo con la normativa interna de seguridad de la información (política, directivas y procedimientos).

8.8. Los colaboradores y contratistas que identifiquen eventos o posibles incidentes en materia de seguridad deben reportarlos a través de la mesa de servicios de TI.

8.9. El incumplimiento de las disposiciones de la presente directiva podría ser pasible del ejercicio de la potestad sancionadora en materia disciplinaria del SENCICO.

9. DISPOSICIONES ESPECÍFICAS

9.1. IDENTIFICAR

9.1.1. SOBRE LA GESTIÓN DE ACTIVOS

9.1.1.1. El Departamento de Informática mantiene un registro de todos los equipos de infraestructura de TI, tanto en entornos on premises como en la nube. Este registro contiene información sobre la descripción, categoría y ubicación de los equipos.

9.1.1.2. Las unidades de organización deben informar con anticipación sobre cualquier requerimiento de cambio, reubicación o manipulación de los equipos de infraestructura de TI al Departamento de Informática, quien evaluará el riesgo y coordinará las acciones a realizar para garantizar el normal desenvolvimiento de las operaciones.

9.1.2. SOBRE LA DISPONIBILIDAD DE LAS INSTALACIONES DE PROCESAMIENTO DE LA INFORMACIÓN

9.1.2.1. El Departamento de Informática gestiona las instalaciones de procesamiento de información con redundancia para cumplir con la disponibilidad requerida por el SENCICO, para lo cual, implementa medidas como la replicación de datos en múltiples ubicaciones y la configuración de sistemas de respaldo, preservando la continuidad operativa y la mitigación ante posibles interrupciones.

9.1.2.2. El Departamento de Informática somete a pruebas periódicas la redundancia de los soportes de los sistemas a fin de garantizar su adecuado funcionamiento evitando posibles casos de conmutación por error entre estos.

9.2. PROTEGER

9.2.1. SOBRE LA GESTIÓN DE IDENTIDAD, AUTENTICACIÓN Y CONTROL DE ACCESO

9.2.1.1. Las unidades de organización son responsables de gestionar la emisión, administración, verificación y revocación de las credenciales de colaboradores, contratistas y equipos de la infraestructura de TI de su unidad.

9.2.1.2. El Departamento de Informática crea identificadores únicos y exclusivos para el uso de los colaboradores y contratistas, a fin de registrar y auditar las actividades de estos.

9.2.1.3. Los colaboradores y contratistas a quienes se le asignen credenciales (cuenta de usuario y contraseña) asumen plena responsabilidad por su uso, estableciéndose claramente que tanto la cuenta de usuario como su contraseña son de carácter personal e intransferible.

9.2.1.4. Los colaboradores y contratistas tienen estrictamente prohibido compartir sus credenciales para su utilización por parte de otras personas, así como, solicitar el restablecimiento de la contraseña de

una cuenta de usuario ajena con el propósito de que sea empleada por otra persona sin importar la justificación (enfermedad imprevista, ausencia laboral, período vacacional, entre otros).

9.2.1.5. El Departamento de Informática sólo asigna privilegios asociados a las cuentas de súper usuario a colaboradores que mantengan un vínculo laboral con el SENCICO y cuya función sea administrar una plataforma específica.

9.2.1.6. El Departamento de Informática realiza la creación de cuentas y asignación de credenciales de cuentas con acceso privilegiado rigiéndose por las siguientes disposiciones:

a) El Departamento de Informática atiende las solicitudes de creación, modificación y/o eliminación de cuentas de súper usuario, las cuales son solicitadas vía el sistema “Solicitud de Accesos a Servicios de Red y Aplicaciones”.

b) El Departamento de Informática registra las acciones de creación, modificación y/o eliminación de las cuentas de súper usuario, indicando lo siguiente:
   - Plataforma de TI 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.

c) El Departamento de Informática guarda las credenciales de las cuentas de súper usuario en sobres sellados y lacrados en la caja fuerte, cuyo contenido debe indicar como mínimo:
   - Plataforma de TI o sistema de información asociado.
   - Nombre de usuario.
   - Contraseña.
   - Ubicación lógica del recurso: IP, URL, esquema, etc.
   - Fecha en que se guardó el sobre.

d) El Departamento de Informática efectúa cambios de contraseña de súper usuario 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 contratistas y los servicios pasan a la administración del SENCICO.
- Cuando es usado por contingencia.
- Cuando se cambia al responsable.

e) El Departamento de Informática define que las contraseñas de súper usuario tienen como mínimo las siguientes características:
- Longitud mínima: Dieciséis caracteres.
- Están compuestas por letras mayúsculas, minúsculas, números, espacios en blanco y caracteres especiales.
- No incluyen caracteres iguales consecutivos.

f) El Asesor en Sistemas e Informática es responsable de llevar a cabo revisiones periódicas de las cuentas con acceso privilegiado con el objetivo de asegurar que los súper usuarios tengan únicamente los privilegios necesarios para desempeñar sus funciones y que no cuenten con privilegios no autorizados, según el reporte semestral elaborado por el Departamento de Informática, a través del Anexo N° 02: Reporte de cuentas con acceso privilegiado.

9.2.1.7. El Departamento de Informática administra y protege los accesos físicos a los activos ubicados en el centro de datos y a los gabinetes de comunicaciones de la Sede Central.

9.2.1.8. Los Gerentes Zonales o Jefes de las Unidades Operativas gestionan y protegen los accesos físicos a los gabinetes de comunicaciones y/o centro de datos de sus respectivas sedes.

9.2.1.9. El Departamento de Informática es responsable de gestionar el acceso remoto a la red interna, así como a las nubes empleadas por el SENCICO.

9.2.1.10. El Departamento de Informática controla que el acceso a la red interna del SENCICO sea a través de VPN y se conceda exclusivamente desde direcciones IP públicas de origen peruano.

9.2.1.11. El Departamento de Informática realiza la segmentación de redes de área local e inalámbricas según niveles de confianza (acceso público, acceso a equipos de cómputo, acceso a servidores, etc.) a unidades de organización u otros.

9.2.1.12. El Departamento de Informática realiza el establecimiento de restricciones entre las VLAN en la capa 3 (IP) y capa 4 (puertos TCP / UDP) para controlar el acceso entre las VLAN, lo cual implica configurar

reglas precisas de enrutamiento y filtrado de puertos para limitar la comunicación solo a la necesaria según las consideraciones de mínimo privilegio.

9.2.1.13. El Departamento de Informática tiene implementadas medidas de protección para las consolas de administración de los dispositivos que gestionan la red LAN/WAN.

9.2.1.14. El Departamento de Informática establece el uso de autenticación de múltiples factores para acceder a los servicios en la nube y sistemas de información que desempeñan un papel crítico para la continuidad de los servicios de TI del SENCICO.

9.2.1.15. El Departamento de Informática implementa las medidas de control para la protección y gestión de accesos de los equipos de red, evitando modificaciones no autorizadas en las configuraciones establecidas.

9.2.1.16. El Departamento de Informática permite el acceso a la red administrativa exclusivamente a equipos y dispositivos móviles de propiedad del SENCICO, así como de colaboradores y contratistas que cuenten con contrato vigente y de visitantes temporales (con acceso restringido a uso de Internet), para lo cual, se necesitará la aprobación de las unidades de organización pertinentes, así como, la revisión y validación por parte del Departamento de Informática para otorgar el acceso solicitado, con la condición de contar con un sistema operativo actualizado y un software antimalware legal, vigente y actualizado, minimizando el riesgo de compromiso de la red.

9.2.1.17. Las unidades de organización a las que pertenecen los colaboradores o los contratistas autorizados para acceder a la red deben solicitar formalmente la creación y el acceso a los servicios y privilegios de la red (correo electrónico, Internet, telefonía IP, sistemas, entre otros) a través del sistema “Solicitud de Accesos a Servicios de Red y Aplicaciones”.

9.2.1.18. El personal de soporte técnico informático y personal autorizado que realiza trabajo a distancia de las unidades de organización son los únicos que tienen permitido el acceso remoto a las estaciones de trabajo dentro de la red interna del SENCICO.

9.2.1.19. El Departamento de Informática mantiene la disponibilidad de los sistemas de información, aplicaciones y servicios de red de lunes a domingo desde las 06:00 hasta las 00:00.

9.2.1.20. El Departamento de Informática configura una contraseña temporal al crearse una cuenta, la cual es forzada a cambiarse a través del sistema operativo al inicio de la primera sesión, luego el colaborador o contratista 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.

9.2.1.21. El Departamento de Informática usa el siguiente estándar para la creación del nombre de una cuenta de correo electrónico y plataforma colaborativa de la parte administrativa: Primera letra del nombre de pila del usuario seguido inmediatamente del apellido paterno ligado por el símbolo “@” al nombre del dominio sencico.gob.pe; en caso de existir dos construcciones de cuenta de usuario similares, se añadirán progresivamente las letras del apellido materno hasta establecer la diferencia. Por ejemplo:

Nombre del usuario: Nombre y Apellido

Nombre de cuenta de correo electrónico: napellido@sencico.gob.pe

9.2.1.22. El Departamento de Informática usa el siguiente estándar para la creación del nombre de una cuenta de correo electrónico y plataforma colaborativa de la parte educativa (alumnos y profesores): Un número autogenerado no repetitivo de 8 dígitos ligado por el símbolo “@” al nombre del dominio sencico.edu.pe. Por ejemplo:

Nombre del alumno: Nombre y Apellido

Nombre de cuenta de correo electrónico: 12345678@sencico.edu.pe

9.2.1.23. El Departamento de Informática crea las cuentas de correo electrónico genéricas, en atención a los requerimientos registrados en el sistema “Solicitud de Accesos a Servicios de Red y Aplicaciones”, habilitando solo las licencias para el funcionamiento del correo electrónico.

9.2.1.24. El Departamento de Informática realiza la creación de cuentas de correo electrónico de los contratistas, usando el nombre estándar que se designará según la información proporcionada por el sistema “Solicitud de Accesos a Servicios de Red y Aplicaciones”.

Se crea de la siguiente manera:

- Las 4 primeras letras (como máximo) que identifica al departamento y/o Gerencia Zonal y/o unidad operativa y/o Centro de formación. Para el caso de la Sede Central se obviará el nombre del departamento de Lima.

- Seguido por un número de dos dígitos

Ejemplos:

abasXX@sencico.gob.pe

tesoXX@sencico.gob.pe

trujXX@sencico.gob.pe

aqpXX@sencico.gob.pe

tiXX@sencico.gob.pe

9.2.1.25. El Departamento de Informática utiliza el siguiente estándar para la creación de una cuenta de usuario de red: 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.

9.2.1.26. El Departamento de Informática gestiona el acceso a los sistemas de información, aplicaciones y servicios de TI del SENCICO solicitados a través del sistema “Solicitud de Accesos a Servicios de Red y Aplicaciones”, lo cual garantiza la asignación adecuada de privilegios y recursos según las responsabilidades y necesidades de cada colaborador o contratista.

9.2.1.27. Las unidades de organización son responsables de llevar a cabo revisiones periódicas de los accesos asignados a los usuarios de su unidad con el objetivo de asegurar que los usuarios tengan únicamente los privilegios necesarios para desempeñar sus funciones y que no cuenten con privilegios no autorizados, según el reporte semestral enviado por el Departamento de Informática, a través del Anexo N° 03: Reporte de privilegios asignados a usuarios

9.2.1.28. El Departamento de Informática remueve o modifica los accesos a los sistemas de información, aplicaciones, servicios de red e instalaciones de procesamiento del SENCICO al momento de la culminación del contrato del colaborador, previa notificación del Departamento de Recursos Humanos o de las unidades de organización, según corresponda. Para el caso de los contratistas, de no existir ninguna solicitud de renovación de acceso o notificación de baja de las cuentas asignadas, se procederá con la baja de las cuentas a los 15 días de culminado el contrato.

9.2.1.29. El Departamento de Informática gestiona la implementación de certificados digitales para garantizar la confidencialidad de la información en las comunicaciones en todas las aplicaciones web.

9.2.1.30. El Departamento de Informática adopta medidas de control para salvaguardar el acceso al código fuente de los sistemas de información o aplicaciones desarrolladas en el SENCICO. Estas medidas incluyen la asignación de permisos de acceso y el control de cambios al código fuente.

9.2.2. SOBRE LA SEGURIDAD DE DATOS

9.2.2.1. El Departamento de Informática protege los datos en reposo a través de la configuración de mecanismos de seguridad en la base de datos tales como: cifrado, enmascaramiento, entre otros.

9.2.2.2. Los datos en tránsito están protegidos de la siguiente manera:

a) El Departamento de Informática configura mecanismos de seguridad de la red para garantizar la transmisión segura de datos, archivos y documentos electrónicos, lo cual es llevado a cabo tanto en la red privada como en la red pública del SENCICO.

b) El Departamento de Informática gestiona los equipos de comunicaciones para proteger la transmisión de datos, archivos y documentos electrónicos en la red privada hacia los servidores de aplicaciones, servidores de bases de datos, servidores de almacenamiento y las estaciones de trabajo de las diferentes dependencias del SENCICO.

c) El Departamento de Informática gestiona las comunicaciones utilizando la red pública para brindar servicios de registros y consultas de datos a terceras partes como alumnos, empresas aportantes, entidades estatales, entre otros.

d) El Departamento de Informática gestiona la transmisión segura mediante el uso de certificados digitales, controles de acceso y otros mecanismos contemplados en la presente directiva.

e) El Departamento de Informática ha configurado los sistemas de información que procesan, almacenan y transmiten datos no públicos para que, durante las operaciones de transferencia de registros electrónicos, archivos, datos, etc., se generen automáticamente registros y pistas de auditoría (audit trails), los cuales contienen información como la fecha, hora y otros datos

relevantes que permiten rastrear y auditar las operaciones realizadas, garantizando la trazabilidad correspondiente.

f) Las unidades de organización establecen acuerdos de transferencia de información con otras entidades que incluyen la administración de responsabilidades para controlar y notificar la transmisión, el despacho y la recepción de la información.

g) El Departamento de Informática implementa los canales seguros de transmisión con otras entidades, en atención a los acuerdos definidos por las unidades de organización.

9.2.2.3. Los colaboradores y contratistas comparten carpetas sólo para fines estrictamente contractuales y si comparten carpetas en su equipo de cómputo asignado, se hacen responsables de la información contenida en ellas y de los privilegios que otorguen a estas a los demás colaboradores y contratistas que acceden la red y plataforma colaborativa.

9.2.2.4. El Asesor en Sistemas e Informática es el único que autoriza el acceso y uso de los programas de utilidad privilegiados en los equipos del SENCICO.

9.2.2.5. El Departamento de Informática mantiene separados los programas de utilidad privilegiados de las aplicaciones regulares, evitando su acceso y uso por parte de colaboradores y contratistas no autorizados.

9.2.2.6. El Asesor en Sistemas e Informática es responsable de verificar que solo los colaboradores y contratistas autorizados por el Departamento de Informática hagan uso de los programas de utilidad privilegiados, a través del Anexo N° 04: Reporte de uso de los programas de utilidad privilegiados.

9.2.2.7. El Departamento de Informática revisa, en coordinación con las unidades de organización, la clasificación y los riesgos de seguridad de la información asociados, para identificar qué datos deben ser cifrados tales como: 1) datos contenidos en información no pública, 2) datos contenidos en registros con credenciales de autenticación, 3) datos contenidos en información no pública almacenada en dispositivos móviles, medios removibles o en soportes de contratistas (servicios de almacenamiento y custodia de copias de respaldo, servicio de almacenamiento en la nube, entre otros) y 4) datos contenidos en

información transferida a través de redes de comunicación no confiables o en medios de almacenamiento físicos no protegidos adecuadamente.

9.2.2.8. El Departamento de Informática gestiona la contratación de proveedores autorizados de certificados digitales para el uso institucional de firmas digitales con el objetivo de asegurar la autenticidad y no repudio de la información en intercambios con otras entidades públicas y otras entidades.

9.2.2.9. El Departamento de Informática especifica dentro de los requisitos de desarrollo de sistemas de información o aplicaciones, que las claves de acceso y los datos no públicos deben ser almacenados de manera cifrada a través del algoritmo criptográfico AES o uno más robusto garantizando que solo aquellos con las claves adecuadas puedan acceder a la información.

9.2.2.10. El Departamento de Informática utiliza algoritmos de cifrado robustos y recomendados por el Ente Rector del Sistema Nacional de Transformación Digital.

9.2.2.11. El Departamento de Informática establece que se deben usar protocolos de acceso remoto seguro para la administración de los equipos tales como SSH (Secure Shell) 2.0 o uno más robusto.

9.2.2.12. El Departamento de Informática establece que se debe usar el protocolo SFTP 2.0, FTPS o uno más robusto para la transferencia segura de archivos.

9.2.2.13. El Departamento de Informática establece que se debe usar el protocolo HTTPS (TLS 1.3) o uno más robusto para la transferencia segura de datos en sistemas de información o aplicaciones web.

9.2.2.14. El Departamento de Informática establece que se debe usar el protocolo IPSEC o uno más robusto para la transferencia segura de datos en las VPN.

9.2.2.15. El Departamento de Informática establece que se debe usar el protocolo S/MIME, PGP o uno más robusto para cifrar y autenticar correos electrónicos, asegurando la privacidad y la integridad de los mensajes.

9.2.2.16. El Departamento de Informática establece que algoritmos criptográficos asimétricos, como RSA, ECDSA o uno más robusto se deben utilizar para crear firmas digitales que autentican la identidad del remitente y garantizan la integridad del contenido.

9.2.2.17. El Departamento de Informática establece que el protocolo de autenticación HMAC o uno más robusto se deben utilizan para verificar

la autenticidad de los mensajes en una red y garantizar la autorización adecuada.

9.2.2.18. El Departamento de Informática establece las redes inalámbricas del SENCICO deben configurarse con un estándar de cifrado seguro, pudiendo ser al menos el WPA3.

9.2.2.19. El Departamento de Informática establece fechas de activación y desactivación para limitar el período de tiempo de uso de las claves criptográficas, las cuales se cambian o actualizan cuando sea necesario, se les realizan copias de respaldo y se protegen contra pérdida o divulgación no autorizada.

9.2.2.20. El Departamento de Informática establece que las claves criptográficas pueden mantenerse en un módulo de criptografía mientras se utilizan, o pueden almacenarse de manera externa con las medidas de seguridad adecuadas y recuperarlas cuando sea necesario.

9.2.2.21. El Departamento de Informática establece que se deben usar módulos de criptografía que se encuentren recomendados y acreditados por estándares como FIPS 140-2, NIST SP, entre otros.

9.2.2.22. El Departamento de Informática establece que se debe proteger la distribución física o electrónica de claves criptográficas según mecanismos establecidos entre el emisor y el receptor. Para la distribución física se puede hacer uso de un mecanismo de cifrado o de CRC, mientras que para la distribución electrónica se puede hacer uso de un mecanismo de cifrado, de MAC o de firma digital.

9.2.2.23. El Departamento de Informática identifica la demanda de capacidad requerida por los sistemas de información y aplicaciones, considerando su criticidad, lo cual implica comprender las necesidades de rendimiento y recursos de los sistemas involucrados.

9.2.2.24. El Departamento de Informática realiza proyecciones de la capacidad de procesamiento, teniendo en cuenta las nuevas necesidades y tendencias.

9.2.2.25. El Departamento de Informática implementa estrategias para administrar la demanda de capacidad como: la eliminación de datos obsoletos, la baja a aplicaciones o sistemas que entren en desuso, optimización de las consultas de bases de datos, entre otros, con la finalidad de proporcionar servicios estables con la capacidad suficiente evitando el consumo innecesario de recursos.

9.2.2.26. El Departamento de Informática usa servicios para la administración de la capacidad de los sistemas y aplicaciones críticas.

9.2.2.27. El Departamento de Informática separa los ambientes de desarrollo, prueba y producción, a través de la implementación de controles de acceso, con el fin de reducir el riesgo de modificaciones no autorizadas en los sistemas de información, aplicaciones y plataformas de TI en producción.

9.2.2.28. El Departamento de Informática establece la segregación de funciones y privilegios para asegurar que solo los colaboradores y contratistas autorizados tengan acceso de modificar los sistemas de información y aplicaciones en cada una de las etapas de su desarrollo, minimizando el riesgo de intrusiones.

9.2.2.29. El Departamento de Informática resguarda los servicios digitales del SENCICO mediante la aplicación de las siguientes medidas de seguridad digital:

a) Uso de mecanismos de autenticación segura.
b) Uso de certificados digitales de seguridad para poder cifrar el canal de comunicación por el que se enviará la información.
c) Uso de cortafuegos de aplicaciones web (WAF, por sus siglas en el idioma inglés) para proteger los servicios de aplicación en redes públicas contra ataques especializados en explotar vulnerabilidades web).
d) Uso de otras tecnologías que puedan favorecer la protección de los servicios digitales.

9.2.2.30. El Departamento de Informática preserva la confidencialidad, integridad y disponibilidad de los datos transmitidos a través de redes públicas mediante el uso de mecanismos, tales como la encriptación de datos en tránsito, controles de autenticación y acceso, monitoreo de actividad sospechosa y firmas de contratos con proveedores de tecnologías de información.

9.2.2.31. El Departamento de Informática mantiene un registro de los dispositivos móviles del SENCICO y su asignación guardando información sobre el identificador del dispositivo móvil, el colaborador o contratista autorizado a quien se le ha asignado, el uso que se le dará al dispositivo móvil, así como el software y hardware requerido por las unidades de organización según el Anexo N° 05: Registro de Asignación de Dispositivos Móviles.

9.2.3. SOBRE LAS CONTRASEÑAS Y SU SEGURIDAD

9.2.3.1. El Departamento de Informática configura las políticas de seguridad del directorio activo para que solicite el cambio automático de contraseña cada 45 días.

9.2.3.2. Los colaboradores y contratistas deben cambiar su contraseña siempre que se sospeche que la seguridad de su contraseña pueda estar comprometida, y también deben informarlo oportunamente al Departamento de Informática para la evaluación correspondiente.

9.2.3.3. El Departamento de Informática determina el formato y sintaxis de las contraseñas bajo los siguientes lineamientos de formato, número de caracteres y tiempo de vida:

• Longitud mínima de 10 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 los patrones de las 12 últimas.

Para la generación de contraseñas seguras, se pueden usar las recomendaciones contenidas en el Anexo N° 06: Recomendaciones para la generación de contraseñas seguras.

9.2.3.4. El Departamento de Informática establece que, para casos donde un colaborador o contratista requiera cambiar una contraseña por pérdida u olvido de esta, éste debe solicitarlo de forma personal a la Mesa de Servicios de TI, quienes deben validar con el colaborador o contratista solicitante el pedido.

9.2.3.5. Los colaboradores o contratistas no deben compartir ni divulgar sus contraseñas o escribirlas en notas, documentos u otros medios, y tampoco difundirlas en conversaciones telefónicas ni de manera presencial.

9.2.3.6. El Departamento de Informática configura la política de seguridad del directorio activo para que, durante el proceso de autenticación el colaborador o contratista tenga tres intentos para ingresar su contraseña correcta, luego de lo cual, la cuenta se bloquea automáticamente y para volver a activar dicha cuenta deberá ponerse en contacto con Mesa de Servicios de TI para el desbloqueo correspondiente.

9.2.3.7. El Departamento de Informática configura la política de seguridad del directorio activo que todos los equipos de cómputo se bloqueen luego de 5 minutos de inactividad, el colaborador o contratista deberá nuevamente autenticarse para volver a tener acceso al sistema.

9.2.3.8. El Departamento de Informática configura, para los casos de los accesos remotos a la red a través de internet, el colaborador o contratista debe realizar doble autenticación: la primera, para establecer el enlace privado con el SENCICO y la segunda, ya estando dentro de la red, para autenticarse como colaborador o contratista autorizado de un sistema de información o servicio de red en particular.

9.2.3.9. Los colaboradores o contratistas, ante situaciones de sustracción o pérdida de información del equipo de cómputo asignado, originado por el compromiso de la cuenta de usuario, son responsables por los daños que pueda causar este hecho a los sistemas de información, aplicaciones, servicios de red, equipos o información del SENCICO. El incidente es evaluado por el Departamento de Informática dentro de su competencia y luego se comunica a la unidad de organización para la evaluación y adopción de las acciones disciplinarias correspondientes.

9.2.4. SOBRE LOS PROCESOS Y PROCEDIMIENTOS DE PROTECCIÓN DE LA INFORMACIÓN

9.2.4.1. El Departamento de Informática dispone de un conjunto de herramientas y sistemas para la administración de los componentes de la infraestructura de TI que se encuentran en el Data Center tales como: sistema de control de accesos, servicio de alimentación ininterrumpida (UPS), flujo de alimentación eléctrica estabilizada, protección del cableado eléctrico, sistema de refrigeración, así como el control del ingreso sólo a los colaboradores del SENCICO o a contratistas autorizados.

9.2.4.2. Los colaboradores del SENCICO a nivel nacional y los contratistas autorizados ingresan al Data Center de acuerdo con el Anexo N° 07: 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 colaboradores del SENCICO a nivel nacional y contratistas 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 colaboradores del SENCICO a nivel nacional y contratistas 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° 08: 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 contratista 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° 08: Bitácora de Acceso al Data Center.

9.2.4.3. El Departamento de Informática designa al colaborador responsable del registro, supervisión, custodia y asistencia de los visitantes autorizados que ingresen al Data Center, en quien recae la responsabilidad del actuar del visitante dentro del área en mención, por lo que su presencia debe ser permanente, a fin de evitar cualquier eventualidad que interrumpa el normal funcionamiento de los equipos de infraestructura de TI ubicados en el Data Center.

9.2.4.4. El Departamento de Informática gestiona los cambios en la configuración de los equipos de infraestructura de TI previa evaluación del impacto operacional y contemplando el retorno a la configuración inicial, de ser el caso.

9.2.4.5. El Departamento de Informática define los controles necesarios para la implementación de cambios en la configuración de los sistemas de información o aplicaciones, minimizando el riesgo a fin no afectar significativamente el buen funcionamiento de estos.

9.2.4.6. El Departamento de Informática gestiona la ejecución de las copias de respaldo de información y pruebas de restauración.

9.2.4.7. El Departamento de Informática cumple con las regulaciones con respecto al entorno operativo físico para los equipos de infraestructura de TI del SENCICO:

a) Gestiona la protección los equipos de comunicaciones que se encuentran instalados en las diferentes Sedes con medidas de

seguridad conocidas (gabinete cerrado con llave y sistema de alimentación continua de energía)

b) Gestiona la ubicación de los equipos de infraestructura de TI del SENCICO en el Data Center y gabinetes de comunicaciones.

c) Gestiona la ubicación de los ambientes del Data Center, así como los gabinetes de comunicaciones (en caso de encontrarse fuera de los ambientes del Data Center) en niveles superiores a donde se ubican los sistemas de agua y desagüe.

d) Gestiona la implementación de los controles de acceso necesarios para el ingreso de los colaboradores del SENCICO y contratistas autorizados al Data Center.

e) Gestiona la implementación de equipos de aire acondicionado para el Data Center, los cuales permiten que los equipos instalados funcionen en las condiciones de temperatura adecuadas.

f) Gestiona la implementación de sistemas de detección y apagado de incendios para el Data Center.

g) Gestiona la implementación de sistemas de monitoreo de las condiciones ambientales de temperatura y humedad del Data Center.

h) Gestiona la protección del cableado de red que transporta datos/voz/video frente a interceptaciones o daños físicos a través de canaletas, gabinetes, entre otros medios.

9.2.4.8. Las unidades de organización gestionan el borrado seguro de la información contenida en los equipos de cómputo de su unidad de manera previa a su reutilización o eliminación, con el fin de eliminar de manera definitiva toda la información no pública almacenada en ellos y evitar posibles riesgos de divulgación no autorizada o acceso no deseado a esta.

9.2.4.9. El Departamento de Informática usa 2 fuentes de sincronización de hora, lo cual es esencial para la investigación de eventos/incidentes que ocurren en la infraestructura, por lo que todos los sistemas de información, aplicaciones y equipos de infraestructura de TI que forman parte de la red del SENCICO se sincronizan a una fuente de tiempo confiable y exacta a través del protocolo NTP.

9.2.5. SOBRE EL MANTENIMIENTO DE EQUIPOS

9.2.5.1. El Departamento de Informática establece el plan de mantenimiento preventivo de los equipos de infraestructura de TI del SENCICO para preservar su disponibilidad e integridad.

9.2.5.2. El Departamento de Informática supervisa los mantenimientos de los equipos de la infraestructura de TI del SENCICO a fin de evitar el acceso no autorizado.

9.2.6. SOBRE LA TECNOLOGÍA DE PROTECCIÓN

9.2.6.1. El Departamento de Informática implementa el principio de Zero trust en la configuración de los recursos de TI que brindan soporte a los sistemas de información y aplicaciones, de manera que ofrezcan únicamente las capacidades esenciales y necesarias, lo cual contribuye a reducir la superficie de ataque y fortalecer la seguridad de los sistemas de información y aplicaciones, al minimizar las posibles vulnerabilidades y riesgos de seguridad de la información asociados.

9.2.6.2. El Departamento de Informática implementa controles de red para mantener la seguridad de la información contra el acceso no autorizado, con el objetivo de salvaguardar la confidencialidad e integridad de los datos que se transmiten a través de redes privadas e inalámbricas utilizadas en el SENCICO.

9.2.6.3. El Departamento de Informática incluye en los términos de referencia para la contratación de bienes y servicios de red, las descripciones de funcionalidades y requisitos de seguridad de la información necesarios tales como el: cifrado, autenticación, tráfico permitido, etc.

9.2.6.4. El Departamento de Informática establece en los términos de referencia para la contratación de bienes y servicios de transmisión de voz y datos de la red del SENCICO, que se debe preservar la seguridad en la transmisión con la mínima cantidad de interrupciones y configurar los equipos de red que interconectan la infraestructura de TI a nivel nacional, los cuales se configuran con rutas establecidas (predefinidas) y dominios lógicos que encaminan el tráfico de la red.

9.2.6.5. El Departamento de Informática autoriza y registra todas las instalaciones, actualizaciones y parches de software en los ambientes de producción, esto incluye la identificación del solicitante, la

descripción del software, la fecha y hora de instalación, y la justificación de la necesidad de instalar el software, según el Anexo N°09: Registro de Instalación de software.

9.2.6.6. El Departamento de Informática sólo permite la instalación de software legal en ambientes de producción proveniente de fuentes confiables y autorizadas por los fabricantes.

9.2.6.7. El Departamento de Informática es el único autorizado a instalar software o establecer líneas de configuración en los ambientes de producción, esto incluye limitar los privilegios de administración.

9.2.6.8. El Departamento de Informática mantiene un registro actualizado del software instalado en los ambientes de producción, esto incluye información detallada sobre las versiones, actualizaciones y parches aplicados, así como las fechas de instalación y los responsables de los cambios.

9.2.7. SOBRE LA SEGURIDAD DE LOS EQUIPOS DE CÓMPUTO

9.2.7.1. El Departamento de Informática gestiona la seguridad de los equipos de cómputo del Data Center del SENCICO a través de las siguientes medidas:

a) Implementando la protección del entorno donde se encuentran los equipos, con perímetros de seguridad definidos, barreras de seguridad y controles de entrada y acceso apropiados.

b) Implementando la protección de los equipos contra pérdidas, daños o compromisos de su seguridad con la finalidad de minimizar los riesgos de interrupciones en las actividades del SENCICO.

9.2.7.2. El Departamento de Informática gestiona la seguridad de los equipos de cómputo que forman parte de la red del SENCICO, a través de las siguientes medidas:

a) El Departamento de Informática controla el acceso de los equipos a las redes internas, externas y a los servicios de red, de forma tal que no comprometa la seguridad de los servicios ofrecidos por el SENCICO.

b) El Departamento de Informática controla el acceso al sistema operativo de los equipos para evitar que, por accesos no autorizados a los equipos, se utilicen las prestaciones de seguridad del propio sistema operativo y haya posibles infiltraciones.

9.2.7.3. Los colaboradores y contratistas son responsables de que los equipos de cómputo sean usados exclusivamente para fines laborales.

9.2.7.4. Los colaboradores o contratistas no deben intentar vulnerar la seguridad digital implementada en el SENCICO.

9.2.7.5. Los colaboradores o contratistas no deben copiar software protegido por derechos de autor en ningún tipo de medio magnético, óptico, repositorio en la nube o similar; es decir, no está autorizada:

a) La copia de los instaladores de software de propiedad del SENCICO. Esto significa que debe ser copiado solamente para fines de respaldo y sólo en caso de estar permitido por la licencia.

b) La instalación de software en equipos del SENCICO que no haya sido autorizada por el Departamento de Informática.

c) La copia de los instaladores de software protegido por derechos de autor usando los equipos del SENCICO. Estas copias sólo pueden ser realizadas por el personal del Departamento de Informática, previa validación de las condiciones de licenciamiento.

9.2.8. SOBRE LA SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

9.2.8.1. Sobre los Entornos de Desarrollo Seguro, el Departamento de Informática, realiza lo siguiente:

a) Gestiona la implementación de un entorno de desarrollo seguro durante todas las etapas del ciclo de vida del desarrollo o mantenimiento de los sistemas de información o aplicaciones, el cual abarca la seguridad en cuanto a las personas, actividades y tecnologías involucradas.

b) Configura los accesos con privilegios mínimos y necesarios a los equipos de desarrollo (tanto interno como externos) a los ambientes de desarrollo.

c) Monitorea los cambios en los ambientes de desarrollo (cambios de configuraciones, cambios de roles o privilegios, entre otros).

d) Realiza las copias de respaldo de los ambientes de desarrollo incluyendo los códigos fuente que allí se almacenan.

9.2.8.2. Sobre la seguridad en el ciclo de vida de desarrollo del software, el Departamento de Informática realiza lo siguiente:

a) El análisis, diseño y pruebas de los requisitos de seguridad de la información establecidos, dentro de los cuales se pueden

considerar: 1) el control de autenticación, 2) el control de roles y privilegios, 3) la segregación de funciones, 4) el registro de auditoría, 5) la seguridad en las comunicaciones, 6) la codificación segura, 7) la elaboración de documentación técnica, 8) la comprobación de configuraciones, 9) las pruebas de requisitos de seguridad del sistema de información, 10) el análisis de vulnerabilidades, 11) la inspección o revisión de código, 12) el enmascaramiento dinámico de datos confidenciales, como datos personales, limitando su exposición según el principio de mínimo privilegio a los usuarios y 13) otros requisitos orientados a los riesgos de seguridad y la información que procesará considerando las amenazas actuales a las que están expuestos.

b) La aplicación de prácticas de codificación segura que se basan en estándares reconocidos a nivel internacional, tales como los documentos estándares de referencia de OWASP Top Ten (riesgos de seguridad más críticos para las aplicaciones web), OWASP Mobile Top 10 (riesgos de seguridad más críticos para las aplicaciones móviles) y OWASP API Security Top 10 (riesgos de seguridad más críticos para las API – Interfaz de Programación de Aplicaciones) y otros similares para otras tecnologías de desarrollo.

9.2.8.3. Sobre los repositorios seguros, el Departamento de Informática realiza lo siguiente:

a) Almacena los códigos fuente generados en repositorios oficiales para mantener la trazabilidad de las modificaciones, los cuales se protegen para que los códigos fuentes no puedan ser accedidos ni modificados de manera no autorizada.

9.2.8.4. Sobre la seguridad en el control de versiones, el Departamento de Informática realiza lo siguiente:

a) Ejerce el control de las versiones de los códigos fuente de los sistemas de información mediante un sistema de control de versiones; esta práctica brinda varios beneficios, incluida la capacidad de restaurar los sistemas a versiones anteriores a la actual, lo que se configura como una medida de contingencia efectiva frente a incidentes o la necesidad de revertir la instalación del sistema de información.

b) Accede al sistema de control de versiones a través de mecanismos de autenticación segura.

9.2.8.5. Sobre la seguridad en las pruebas de sistemas de información

Se tienen las siguientes disposiciones:

a) El Departamento de Informática diseña y realiza pruebas funcionales y no funcionales sobre los requisitos de seguridad de la información definidos en la disposición 9.2.8.2 - a) para los sistemas de información.

b) El Departamento de Informática realiza la transferencia de los sistemas de información desde el ambiente de desarrollo al ambiente de prueba y del ambiente de prueba al ambiente de producción de manera segura.

c) Los colaboradores que vayan a usar los sistemas de información y aplicaciones desarrollados deben realizar las pruebas de aceptación de estos en los ambientes de prueba de manera guiada por el Departamento de Informática, en las funcionalidades desarrolladas.

9.2.8.6. Sobre el conocimiento en seguridad de sistemas de información

a) El Departamento de Informática gestiona con el Departamento de Recursos Humanos que el personal que integra el equipo de desarrollo cuente con las competencias requeridas en principios y buenas prácticas de seguridad de sistemas de información, y adicionalmente, determina las necesidades de capacitación del personal, las cuales deben ser cubiertas por el SENCICO o establecerse como requisitos de los equipos de desarrollo cuando van a ser provistos por contratistas para el desarrollo o mantenimiento de sistemas de información o aplicaciones.

9.2.8.7. Sobre la revisión técnica después de cambios a la plataforma operativa

Se tienen las siguientes disposiciones.

a) El Departamento de Informática lleva a cabo revisiones técnicas de todos los sistemas de información o aplicaciones después de realizar cambios en la plataforma operativa donde están alojados, para asegurar que no haya impactos adversos en las operaciones o la seguridad de la información y que los sistemas de información o aplicaciones continúen funcionando correctamente.

9.2.8.8. Sobre las restricciones sobre cambios a los paquetes de software, el Departamento de Informática considera lo siguiente:

a) Configura las restricciones de control de accesos a los repositorios que contienen los paquetes de software para evitar que se realicen modificaciones no autorizadas.
b) Realiza pruebas en los entornos de desarrollo y pruebas, antes de implementar cualquier cambio en los paquetes de software para verificar que no se introduzcan vulnerabilidades o problemas de seguridad.
c) Mantiene un registro de los cambios realizados en los paquetes de software, incluyendo la justificación del cambio, la fecha de implementación y los responsables de la realización del cambio, según el Anexo N° 10: Registro de Cambios de Paquetes de Software.

9.2.8.9. Sobre el desarrollo contratado externamente, el Departamento de Informática tiene en consideración lo siguiente:
a) Establece en los términos de referencia los requisitos de seguridad para el desarrollo de software, para la contratación de proveedores de servicios de desarrollo y mantenimiento de sistemas de información y aplicaciones.
b) Supervisa el cumplimiento de las cláusulas contractuales de seguridad para el desarrollo y pruebas de software con los proveedores externos de servicios de desarrollo y mantenimiento de sistemas de información y aplicaciones para garantizar la seguridad del software desarrollado.

9.2.8.10. El Departamento de Informática vela por que no haya información personal identificable o cualquier otro tipo de información no pública en los ambientes de desarrollo o pruebas.

9.3. DETECTAR

9.3.1. SOBRE ANOMALÍAS Y EVENTOS

9.3.1.1. El Departamento de Informática utiliza herramientas basadas en inteligencia artificial y aprendizaje automático para establecer las bases de referencia para las operaciones de red y los flujos de datos esperados para los usuarios y sistemas.

9.3.1.2. El Departamento de Informática mantiene los registros de eventos guardando como mínimo los siguientes parámetros:
- Identificación del usuario y/o equipo.
- Fecha y hora del evento.

- Acciones efectuadas.

9.3.1.3. El Departamento de Informática mantiene y revisa con regularidad los registros de eventos de usuarios y administradores para el seguimiento de eventos o posibles incidentes de seguridad, para que ante cualquier hallazgo o incidente relevante éste sea investigado y tratado de acuerdo con el procedimiento establecido para tal fin.

9.3.1.4. El Departamento de Informática monitorea los servicios de seguridad digital, a través de consolas que gestionan las políticas de seguridad que se han configurado.

9.3.2. SOBRE EL MONITOREO CONTINUO DE LA SEGURIDAD

9.3.2.1. El Departamento de Informática monitorea constantemente el tráfico de la red de telecomunicaciones para la detección de eventos o posibles incidentes de seguridad.

9.3.2.2. El Departamento de Informática analiza los intentos de accesos no autorizados de las cuentas de los colaboradores o contratistas a los sistemas de información o aplicaciones a fin de detectar eventos o posibles incidentes de seguridad.

9.3.2.3. El Departamento de Informática dispone de herramientas que detectan automáticamente las posibles infecciones por software malicioso.

9.3.2.4. El Departamento de Informática supervisa regularmente la actividad de los proveedores de servicios externos para detectar eventos o posibles incidentes de seguridad.

9.3.2.5. El Departamento de Informática cuenta con un servicio de evaluación automática y continua de vulnerabilidades en todos los servicios implementados en la nube pública para detectar eventos o posibles incidentes de seguridad.

9.3.2.6. El Departamento de Informática identifica la conexión de cualquier dispositivo informático no autorizado para detectar eventos o posibles incidentes de seguridad.

9.3.3. SOBRE LA PROTECCIÓN CONTRA ATAQUES INFORMÁTICOS, SOFTWARE MALICIOSO Y SIMILARES

9.3.3.1. El Departamento de Informática implementa equipos y servicios de seguridad perimetral de alta disponibilidad como son: NGFW, WAF, AntiDDoS, EDR y similares, para restringir los accesos externos a los servicios y aplicaciones web que publica el SENCICO.

9.3.3.2. El Departamento de Informática gestiona la implementación de consolas para la administración de los equipos de seguridad perimetral, para la configuración de las políticas de seguridad y las reglas de acceso definidas para cada uno de estos equipos.

9.3.3.3. El Departamento de Informática gestiona la protección de seguridad de los puertos de switches de borde limitando el tráfico en los puertos solo a lo mínimo necesario, deshabilitando los puertos no usados, estableciendo una autenticación sólida a los puertos para que solo los dispositivos y usuarios autorizados puedan conectarse, limitando la tasa de tráfico permitido en corto tiempo en los puertos, protegiendo los puertos contra el acceso remoto, así como, actualizando el firmware y las configuraciones de seguridad de los switches.

9.3.3.4. El Departamento de Informática cuenta con servicios de retención de logs, donde se registran los accesos y eventos que son generados por cada uno de los equipos y servicios de seguridad implementados.

9.3.3.5. Los colaboradores o contratistas autorizados acceden a las herramientas y servicios de monitoreo y administración de la red usando doble factor de autenticación.

9.3.4. SOBRE LA PROTECCIÓN CONTRA SOFTWARE MALICIOSO

9.3.4.1. El Departamento de Informática gestiona la configuración de la solución de EDR, para la protección de los equipos de cómputo y los servidores en tiempo real contra el software malicioso, la cual gestiona simultáneamente los siguientes niveles de protección a través de una consola web centralizada:

a) 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.

b) Nivel de Internet y cliente de correo electrónico: Para la protección de la navegación en internet y el correo electrónico.

9.3.4.2. El Departamento de Informática gestiona la configuración de las soluciones de protección del correo electrónico, ofrecido por el servicio de correo electrónico y plataforma colaborativa.

9.3.4.3. El Departamento de Informática configura la solución EDR para detectar los eventos y posibles incidentes originados por la conexión de dispositivos USB que usan los colaboradores y contratistas autorizados.

9.3.4.4. El Departamento de Informática, evalúa las solicitudes de habilitación de puertos USB realizadas por las unidades de organización.

9.3.4.5. El Departamento de Informática gestiona la implementación de soluciones EDR y otros mecanismos en los dispositivos móviles de propiedad del SENCICO (dependiendo su aplicación según el tipo de dispositivo).

9.3.4.6. El Departamento de Informática evalúa los eventos o posibles incidentes causados por infecciones de software malicioso por el uso de dispositivos USB por parte de los colaboradores o contratistas autorizados y de ser el caso, comunicará a las unidades de organización competentes para la adopción de las medidas disciplinarias en caso de corresponder.

9.3.4.7. El Departamento de Informática implementa las capacidades de filtrado de software malicioso, phishing y spam en el servicio de correo electrónico y plataforma colaborativa.

9.3.4.8. El Departamento de Informática configura la creación de listas blancas (remitentes/destinatarios permitidos) y listas negras (remitentes/destinatarios prohibidos) para el servicio de correo electrónico institucional.

9.3.4.9. El Departamento de Informática gestiona la configuración de opciones de filtro de contenido web en los equipos de seguridad perimetral para restringir la navegación por páginas web con contenido malicioso.

9.3.4.10. Los colaboradores y contratistas autorizados no deben descargar archivos y/o programas (software gratuito) ejecutables (*.exe, *.msi, *.dll, etc.) en su formato original o comprimido (*.zip, *.rar, etc.), archivos de música, video en todos sus formatos (*.mp3, *.wav, *.mp4, etc.), entre otros.

9.3.4.11. El Departamento de Informática está facultado a tomar el control físico o remoto de los equipos de cómputo donde se haya detectado una infección por software malicioso o propagación en progreso, a fin de controlar y mitigar sus efectos.

9.3.5. SOBRE LA GESTIÓN DE VULNERABILIDADES TÉCNICAS

9.3.5.1. El Departamento de Informática realiza evaluaciones periódicas de las vulnerabilidades técnicas de los sistemas y aplicaciones críticas, a fin de determinar si existen vulnerabilidades que puedan ser explotadas por atacantes externos o internos, la cual comprende las siguientes

actividades: la determinación del alcance de la evaluación, el análisis de vulnerabilidades y/o pruebas de intrusión, prueba y mitigación de las vulnerabilidades y el seguimiento de las vulnerabilidades técnicas.

9.3.5.2. El Departamento de Informática establece la urgencia y priorización de los planes de acción para la remediación de las vulnerabilidades técnicas detectadas durante las evaluaciones y sus plazos, sobre la base de las características, impacto y severidad de las vulnerabilidades calculadas según el estándar CVSS 3.0 o superior.

9.3.5.3. El Departamento de Informática gestiona la aplicación de parches de seguridad en los sistemas de información y aplicaciones considerando: el monitoreo e identificación de las vulnerabilidades técnicas a mitigar, análisis de los riesgos asociados a la aplicación del parche, las pruebas de los parches y el despliegue o mitigaciones temporales a cada uno de los activos informáticos.

9.3.6. SOBRE LA REVISIÓN DEL CUMPLIMIENTO TÉCNICO

9.3.6.1. El Departamento de Informática coordina las revisiones periódicas de cumplimiento técnico de los sistemas de información o aplicaciones con la normativa interna de seguridad.

9.3.6.2. El Departamento de Informática contempla la ejecución de análisis de vulnerabilidades en los sistemas de información y aplicaciones para complementar las revisiones periódicas de cumplimiento técnico con la normativa interna de seguridad.

9.3.7. SOBRE LAS RESTRICCIONES DE INSTALACIÓN DE SOFTWARE

9.3.7.1. Los colaboradores y contratistas autorizados del Departamento de Informática, los cuales están registrados usando el Anexo N° 11: Registro de Personal Autorizado a la Instalación de Software Corporativo del SENCICO, son los únicos que están permitidos de instalar software licenciado corporativo en los equipos de cómputo del SENCICO.

9.4. RESPONDER

9.4.1. SOBRE LA PLANIFICACIÓN DE LA RESPUESTA

9.4.1.1. Los colaboradores que componen el CSIRT planifican la atención a los incidentes de seguridad digital notificados o identificados, según el procedimiento de atención de incidentes de seguridad digital.

9.4.2. SOBRE LAS COMUNICACIONES

9.4.2.1. El Departamento de Informática recibe notificaciones de posibles incidentes de seguridad de la información de tipo digital e identifica alertas y reportes generados por las herramientas de monitoreo o consolas de gestión, y en caso de que estos escalen y califiquen como incidente de seguridad digital, son comunicados al CSIRT.

9.4.2.2. El CSIRT informa al Centro Nacional de Seguridad Digital los incidentes de acuerdo con los criterios establecidos.

9.4.3. SOBRE EL ANÁLISIS

9.4.3.1. El CSIRT recopila evidencias de los incidentes de seguridad digital identificados y evalúa el impacto inicial del incidente, según el procedimiento de atención de incidentes de seguridad digital.

9.4.3.2. El Departamento de Informática usa el conocimiento de las vulnerabilidades divulgadas al SENCICO por los grupos de interés (medios o investigadores especializados que envían actualizaciones, avisos de alertas, noticias o boletines de seguridad de la Información), para prevenir y mitigar incidentes de seguridad.

9.4.3.3. El CSIRT coordina la mejora los mecanismos de protección de la infraestructura de TI, desde el aprendizaje de los incidentes de seguridad digital.

9.4.4. SOBRE LA MITIGACIÓN

9.4.4.1. El CSIRT coordina la ejecución de las acciones propuestas en el formato de registro de incidentes del procedimiento de atención de incidentes de seguridad digital, a fin de contener o mitigar el incidente de seguridad digital.

9.4.5. SOBRE LAS MEJORAS

9.4.5.1. El CSIRT documenta las lecciones aprendidas, que son incluidas en el acta de sesión del CSIRT.

9.4.5.2. El CSIRT actualiza las estrategias de respuesta.

10. ANEXOS

- **Anexo N° 01:** Matriz de Contacto con Grupos de Interés
- **Anexo N° 02:** Reporte de cuentas con acceso privilegiado
- **Anexo N° 03:** Reporte de privilegios asignados a usuarios
- **Anexo N° 04:** Reporte de uso de los programas de utilidad privilegiados
- **Anexo N° 05:** Registro de Asignación de Dispositivos Móviles
- **Anexo N° 06:** Recomendaciones para la generación de contraseñas seguras
- **Anexo N° 07:** Instructivo de Seguridad y Correcto Uso de las Instalaciones de Procesamiento de la Información
- **Anexo N° 08:** Bitácora de Acceso al Data Center
- **Anexo N° 09:** Registro de Instalación de software
- **Anexo N° 10:** Registro de Cambios de Paquetes de Software
- **Anexo N° 11:** Registro de Personal Autorizado a la Instalación de Software Corporativo del SENCICO

ANEXO N° 01

MATRIZ DE CONTACTO CON GRUPOS DE INTERÉS

	MATRIZ DE CONTACTO CON GRUPOS DE INTERÉS

N°	Nombre de la entidad	Descripción de la entidad	Contactos de la entidad	Medios de contacto con la entidad	Materias involucradas
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

ANEXO N° 02

REPORTE DE CUENTAS CON ACCESO PRIVILEGIADO

		REPORTE DE CUENTAS CON ACCESO PRIVILEGIADO						
N°	**Servicio**	**Rol (Administrador, usuario, otros)**	**Nombre de la cuenta**	**Plataforma Tecnológica**	**Unidad, Área o Empresa**	**Fecha de creación**	**Fecha de desactivación**	**Estado**

Fecha de reporte: XX/XX/20XX

ANEXO N° 03

REPORTE DE PRIVILEGIOS ASIGNADOS A USUARIOS

	REPORTE DE PRIVILEGIOS ASIGNADOS A USUARIOS								
N°	**Sistema de Información**	**Perfil de la cuenta**	**Privilegiados asignados a la cuenta**	**Nombre de la cuenta**	**Usuario(s) asignados a la cuenta**	**Unidad, Área o Empresa**	**Fecha de creación**	**Fecha de desactivación**	**Estado**

ANEXO N° 04

REPORTE DE USO DE LOS PROGRAMAS DE UTILIDAD PRIVILEGIADOS

	REPORTE DE USO DE LOS PROGRAMAS DE UTILIDAD PRIVILEGIADOS

N°	Componente(s) de Infraestructura de TI	Programa de utilidad privilegiado	Sistema(s)/Usuario(s) que acceden	Razón o Justificación del uso

Anexo N° 05

REGISTRO DE ASIGNACIÓN DE DISPOSITIVOS MÓVILES

	REGISTRO DE ASIGNACIÓN DE DISPOSITIVOS MÓVILES

N°	N° de Serie	Tipo de dispositivo móvil	Colaborador / Contratista	Unidad de organización	Uso del dispositivo móvil	Software o hardware requerido

Anexo N° 06

Recomendaciones para la generación de contraseñas seguras

1. **Definir un nemotécnico de 4 o más letras**
   a. Que no sea una palabra que tenga significado en algún diccionario.
   b. Debe tener un significado para ti, de tal forma que lo puedas recordar. Por ejemplo:
   lqevsll, significa "**l**o **q**ue **e**l **v**iento **s**e **ll**evó"
   pelvmten, significa "**p**uedo **e**scribir **l**os **v**ersos **m**ás **t**ristes **e**sta **n**oche"

2. **Definir un nemotécnico de 4 o más letras**
   a. Que tenga un significado emocional para ti.
   Por ejemplo:
   1408, puede significar 14 de agosto
   1075, puede significar octubre del año 75
   4720, puede significar la dirección de la primera casa en la que viví

3. **Seleccionar 1 carácter especial**
   a. Escoger un carácter especial. Puede ser: $, %, #

4. **Escoger 2 caracteres de la aplicación de la cual somos usuarios**
   a. Escoger dos caracteres de la aplicación que usamos o vamos a usar.
   b. Los 2 caracteres pueden ser los 2 primeros, los dos últimos, o el primero y el último.
   c. Los 2 caracteres los vamos a usar en mayúscula.

   Ejemplo, si decidimos trabajar con los 2 primeros caracteres:

   Para Facebook, será: FA
   Para LinkedIn, será: LI
   Para Gmail, será: GM

5. **Generar contraseñas**
   Finalmente, se pueden generar las siguientes combinaciones de contraseñas, dependiendo del tipo de plataforma:

   Gmail: GM$lqevsll$1408 o lqevsll1408GL
   LinkedIn: Ll$lqevsll$1408 o lqevsll1408LN
   Netflix: NE$lqevsll$1408 o lqevsll1408NX
   Airbnb: Al$lqevsll$1408 o lqevsll1408AB

ANEXO N° 07

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 contratistas no autorizados 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.

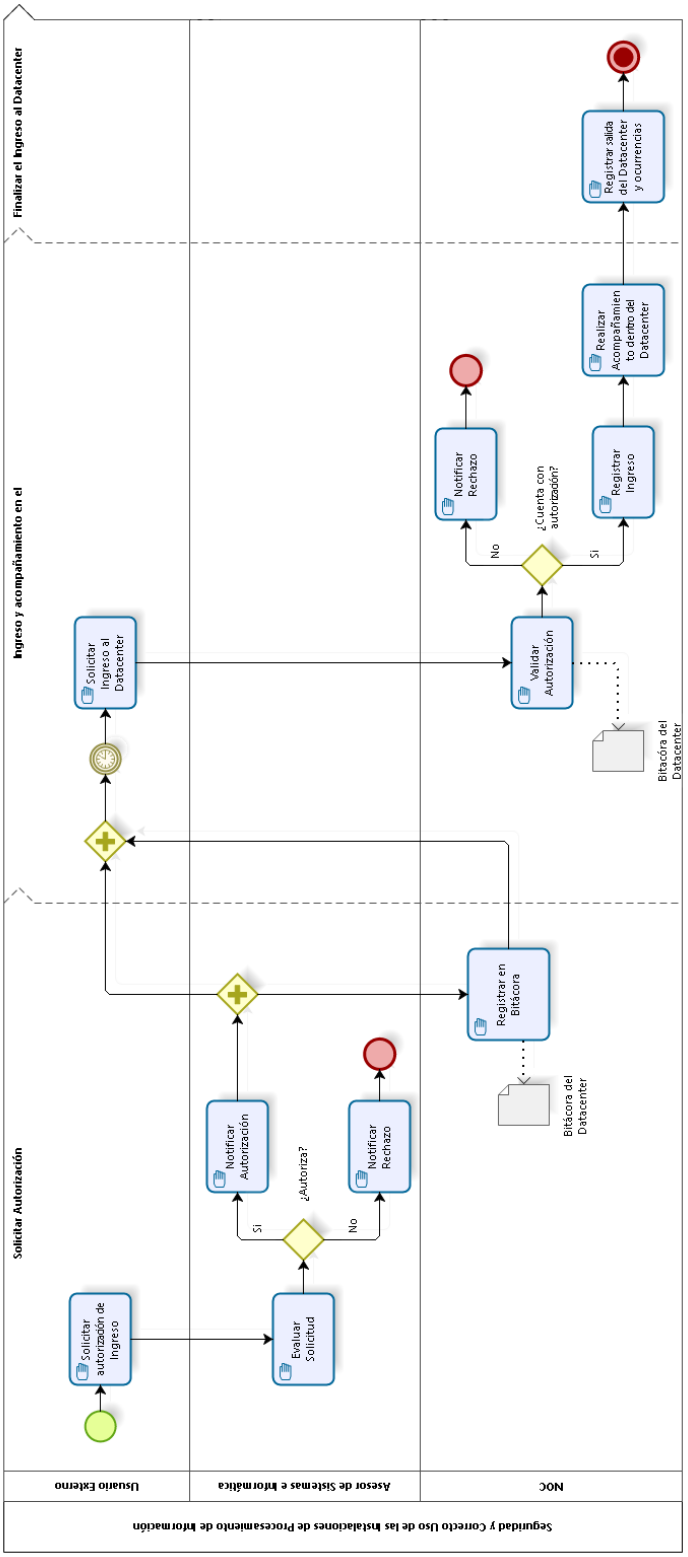
5. DEFINICIONES

- **Tecnología de Información (TI):** Se refiere al hardware y software operados por la Institución o por un contratista 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 Data center 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 Data center	Solicita ingreso al Data center.	Usuario Externo		5 min

N°	Actividad	Descripción	Responsable	Registro	Tiempo
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		
9	Registrar ingreso		Responsable del NOC	Bitácora	5 min
10	Realizar acompañamiento dentro del Data center	Realiza acompañamiento a la visita durante su estadía en el Data center.	Personal del NOC		--
11	Registrar salida del Data center y ocurrencias	Registra la salida del Data center 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° 08

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° 09

REGISTRO DE INSTALACIÓN DE SOFTWARE

SENCICO SERVICIO NACIONAL DE CAPACITACIÓN PARA LA INDUSTRIA DE LA CONSTRUCCIÓN	**REGISTRO DE INSTALACIÓN DE SOFTWARE**

N°	Usuario Solicitante	Descripción de Software	Versión de Software	Tipo de Instalación	Justificación de la Instalación	Fecha y Hora de Instalación	Responsable de la Instalación

(*) Tipo de Instalación: Inicial, Actualización, Parche

Anexo N° 10

REGISTRO DE CAMBIOS DE PAQUETES DE SOFTWARE

	REGISTRO DE CAMBIOS DE PAQUETES DE SOFTWARE

N°	Usuario Solicitante	Descripción del Paquete	Versión del Paquete	Descripción del cambio	Justificación del cambio	Fecha de Implementación	Responsable de Implementación

Anexo N° 11

REGISTRO DE PERSONAL AUTORIZADO A LA INSTALACIÓN DE SOFTWARE CORPORATIVO DEL SENCICO

	REGISTRO DE PERSONAL AUTORIZADO A LA INSTALACIÓN DE SOFTWARE CORPORATIVO DEL SENCICO

N°	Colaborador/Contratista	Puesto	Unidad de Organización	Sede	Datos de contacto	Tipo de software corporativo permitido para instalar	Fecha de autorización