al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red del Equipo Funcional de Tecnologías de la Información.

e) La contraseña no debe hacer referencia a ningún concepto, objeto o idea reconocible. Por tanto, se debe evitar utilizar en las contraseñas fechas significativas, días de la semana, meses del año, nombres de personas, teléfonos.
f) En caso que el sistema no lo solicite automáticamente, el usuario debe cambiar la contraseña provisional asignada la primera vez que realiza un acceso válido al sistema como medida de seguridad.
g) En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada tres meses. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.
h) Utilizar el menor número de listados que contengan datos de carácter personal y mantener los mismos en un lugar seguro y fuera del alcance de terceros.
i) Las contraseñas deberán tener por lo menos dos caracteres numéricos y una letra mayúscula.
j) No deberá utilizar contraseñas utilizadas anteriormente.
k) No se recomienda utilizar la misma contraseña para todos los sistemas que utilice el usuario.

8.2.16. Uso Apropiado de los Recursos

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para complementar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho confidencialidad en su uso.

8.2.16.1. Queda Prohibido

a) El uso de estos recursos para actividades no relacionadas con el propósito de la institución, o bien con la extralimitación en su uso.
b) Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de la Institución.
c) Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
d) Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.
e) Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos programas o documentos electrónicos.

f) Albergar datos de carácter personal en las unidades locales de disco de computadores de trabajo.

8.2.17. Antivirus

8.2.17.1. Antivirus de Red

a) Todos los equipos de cómputo de la Institución deberán tener instalada un Solución Antivirus.
b) Periódicamente se hará el rastreo en los equipos de cómputo de la Institución, y se realizará la actualización de las firmas de antivirus proporcionadas por el fabricante de la solución antivirus en los equipos conectados a la Red.

8.2.17.2. Responsabilidad de los Administradores de Red

Los Administradores de Red serán responsables de:

a) Implementar la Solución Antivirus en los equipos informáticos de la Institución, esto incluye, equipos de cómputo, servidores, laptops y tabletas, independiente del sistema operativo que utilicen.
b) Solucionar contingencias presentadas ante el surgimiento de virus que la solución no haya detectado automáticamente.
c) Configurar el analizador de red para la detección de virus.
d) Configurar adecuadamente el servidor de definición de virus, para que distribuya de manera automática los paquetes de actualización a todos los equipos de la institución.
e) Asegurarse que el servidor de definición de virus este actualizándose de solución de seguridad de antivirus integra las herramientas Antivirus, o antispyware, firewall y prevención contra intrusiones, además de control de dispositivos y aplicaciones usando un único agente multiplataforma (Windows, Linux) para todos los clientes y gestionado mediante una consola central.

DIRIS LIMA CENTRO · Oficina de Tecnologías de Información · V°B°

DIRIS LIMA CENTRO · Oficina de Planeamiento y Modernización · V°B°

8.2.17.3. Uso del Antivirus por los Usuarios

a) El usuario no deberá intentar desinstalar o manipular la solución antivirus de su computadora pues ocasiona un riesgo de seguridad ante el peligro de virus.
b) Si el usuario hace uso de medios de almacenamiento personales, éstos serán rastreados por la Solución Antivirus en la computadora del usuario o por el equipo designado para tal efecto.
c) El usuario deberá comunicarse con Los Técnicos de Soporte en caso de problemas de virus para buscar la solución.
d) El usuario será notificado por los Administradores de Red en los siguientes casos:
   - Cuando sea desconectado de la red con el fin evitar la propagación del virus a otros usuarios de la dependencia.

- Cuando sus archivos resulten con daños irreparables por causa de virus.
- Cuando viole las políticas antivirus.

8.2.17.4. Políticas Antivirus

Todos los equipos de cómputo conectados a la red corporativa deben tener instalado y debidamente actualizado el antivirus, con el fin de que esto sea cumplido. Cualquier proceso interno de asignación o rotación de equipos de cómputo le corresponde una lista de chequeo para su alistamiento, lista dentro de la cual se encuentra debidamente registrado la instalación o validación del antivirus.

8.2.17.5. Control de Aplicaciones y Dispositivos

a) Conjunto de reglas que permiten controlar acceso de aplicaciones y/o dispositivos a los recursos del sistema, con el fin de prevenir riesgos de infección y/o seguridad.
b) Bloqueo a ejecución de aplicaciones desde CD-ROM/DVD-ROM y dispositivos de almacenamiento removibles incluyendo Autorun.inf.
c) Las aplicaciones desarrolladas por la Institución deberán tener, por lo menos, con contraseña al inicio para permitir la entrada de los usuarios a éstas.
d) Las soluciones desarrolladas en la institución deberán tener perfiles de usuario, estos perfiles permitirán darle los mínimos permisos de acceso para que pueda realizar sus tareas. Cualquier tarea de administración de usuario que implique eliminación de datos, el sistema deberá de pedir al usuario su login y contraseña.
e) El sistema deberá de realizar solo borrados lógicos y no físicos de los datos.
f) Las acciones de inicio de sesión, cierre de sesión, ingreso, actualización y borrado de datos debe de quedar registrado en los logs del sistema.

8.3. Políticas de Control de Acceso

a) Se debe controlar el acceso de la información y los procesos del negocio sobre la base de los requisitos de seguridad de la institución.
b) Se debe controlar y prevenir el acceso no autorizado a los servicios de las redes internas y externas, así como también en los sistemas de aplicación.
c) El personal debe ser consciente de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, principalmente en el uso de contraseñas y a la seguridad de recursos puestos a su disposición.
d) Todo el personal debe cumplir con la norma de pantalla bloqueada para reducir el riesgo de acceso no autorizado o de daños a los papeles, medios e instalaciones de procesamiento de información.

Tipo de Documento	Numeración	Siglas de la Institución	Año calendario de Aprobación	Sigla del Órgano que genera el DN
DIRECTIVA ADMINISTRATIVA	001	DIRIS LC	2021	OTI-DA DIRIS-LC V01

8.3.1. Requerimiento Para Control De Acceso

Todos los accesos a los recursos de información de la DIRIS LIMA CENTRO deben basarse en la necesidad y rol del usuario, debiendo tomarse en cuenta los siguientes aspectos:

a) Los requerimientos de seguridad de cada una de las aplicaciones.
b) Identificación de toda la información relacionada a las aplicaciones y riesgos a la que está expuesta.
c) Coherencia entre las políticas de control de acceso y las políticas de clasificación de la información.
d) Uso de perfiles de usuarios definidos por roles, los mismos que deberán otorgar el mínimo número de privilegios para que puedan realizar sus tareas.
e) Revisión periódica de los controles de acceso.
f) Revocación de los controles de acceso.

8.3.2. Gestión de Acceso al Personal

a) Con el propósito de impedir accesos no autorizados a los recursos de información, deben establecerse procedimientos formales para asignar los derechos de acceso a los sistemas.
b) Los funcionarios son los encargados de autorizar y solicitar el acceso del personal a su cargo a los recursos de tecnología de información, conforme al procedimiento que se establezca para tal efecto.
c) Deben definirse normas y procedimientos de control a nivel de sistema operativo de red, de manera que no compartan indicadores entre diferentes usuarios ni pueda detectarse la duplicidad de sesiones de usuarios.
d) Los usuarios deben bloquear su estación de trabajo si por algún motivo se retiran de su puesto de labores.
e) Todas las estaciones de trabajo deben tener un protector de pantalla con clave y activación automática de bloqueo de usuario, cuando no se estén utilizando.
f) El personal debe mantener sus escritorios libres de documentos y/o medios de almacenamiento removibles, cuando no los utilicen, procurar guardarlos en gabinetes con llaves cuando se retiren del centro de labores.

8.3.3. Red Inalámbrica (WIFI)

8.3.3.1. Acceso a Funcionarias de la Institución

a) La red inalámbrica es un servicio que permite conectarse a Internet sin la necesidad de algún tipo de cableado. La Red inalámbrica le permitirá utilizar los servicios de Red, en las zonas de cobertura de la Institución.
b) Donde además de hacer uso del servicio de acceso a los sistemas, podrán acceder al servicio de Internet de manera controlada.
c) Los Administradores de Red, son los encargados de la administración, habilitación o

d) bajas de usuarios en la red inalámbrica de la Institución.
e) La solicitud de acceso a la red inalámbrica debe de ser realizada de manera formal, a través del llenado de un formato.

8.3.3.2. Restricciones/Prohibiciones De Acceso A Internet

Con la finalidad de hacer un buen uso de la red inalámbrica, se aplicarán las siguientes restricciones:

a) El acceso a páginas con cualquier tipo de contenido explícito de pornografía o material de carácter ofensivo.
b) El uso de sitios de videos en línea o en tiempo real.
c) Uso de juegos "on-line" en la red.
d) No se permite la conexión a estaciones de radio por Internet.
e) No se permite el acceso a páginas con contenido de streaming o trasmisión de videos, tipo YouTube.
f) No se permite el acceso y uso de sitios web de descarga de contenidos, ni el uso de aplicaciones que permitan las descargas de contenidos tipo torrent, ares, edonkey y similares.

8.3.3.3. Excepciones

a) Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.
b) En caso de eventos, cursos, talleres, conferencias, etc., se podrán habilitar equipos con acceso a la red inalámbrica de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil.
c) En el caso de estos eventos las restricciones para acceder podrán ser "anuladas" temporalmente previa solicitud expresa por parte de la parte interesada y con anticipación de por lo menos un día hábil.

8.3.3.4. Acceso a Invitados

a) La red inalámbrica (INVITADOS- DIRIS LIMA CENTRO) es un servicio que permite conectarse única y exclusivamente a personal externo de la Institución (clientes, proveedores) a internet sin la necesidad de algún tipo de cableado. La Red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura de la Institución.
b) Los usuarios invitados no tendrán acceso a la Red de La Institución o algún recurso de uso privado de La Institución.
c) La red inalámbrica (INVITADOS - DIRIS LIMA CENTRO) tendrá un perfil de carácter restringido, permitiendo el acceso solo a sitios web de carácter

institucional y que estén relacionado con las actividades que los usuarios realizarán durante su estadía en la DIRIS LIMA CENTRO.

8.4. Políticas de Adquisición, Desarrollo y Mantenimiento de Software

La seguridad en los sistemas de información debe estar incluida en la infraestructura tecnológica, las aplicaciones desarrolladas internamente y las aplicaciones desarrolladas por terceros para la institución.

Los requisitos de seguridad y derecho de autor deben ser identificados y consensuados antes de desarrollar los sistemas de información.

Se deben diseñar dentro de las aplicaciones de medidas de control que deben incluir la validación de los datos de acceso, entrada, el tratamiento interno y datos de salida.

Se debe requerir controles adicionales para sistemas que procesen o tengan impacto en información sensible, con mucho valor o critica. Estos Controles deben ser determinados en base a los requisitos de seguridad y una evaluación de riesgos.

Se debe controlar el acceso a los archivos del sistema y proyectos información, así como las actividades complementarias que deben ser llevadas a cabo de forma segura.

Se debe asegurar la revisión de todo cambio propuesto al sistema para comprobar que no debilite su seguridad o la del sistema operativo.

Los sistemas deben de soportar el registro de logs sobre las acciones de los usuarios, además de registrar campos de auditoría en cada una de las transacciones que realiza.

9.5. Adquisición

Toda adquisición de tecnología informática se efectuará a través del Comité de Gestión de la Seguridad de la Información. El EFTIC será la responsable de planear las operaciones relativas a la adquisición de bienes informáticos, establecerán prioridades y en su selección deberá tomar en cuenta:

9.5.1. Precio

Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.

9.5.2. Calidad

Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.

Tipo de Documento	Numeración	Siglas de la Institución	Año calendario de Aprobación	Sigla del Órgano que genera el DN
DIRECTIVA ADMINISTRATIVA	001	DIRIS LC	2021	OTI-DA DIRIS-LC V01

9.5.3. Experiencia

Estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.

9.5.4. Presencia en el Mercado

Expresado en el tiempo que la marca se encuentra en el mercado peruano. El área de cobertura de su soporte técnico y garantía a nivel nacional.

9.5.5. Desarrollo Tecnológico

Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.

9.5.6. Estándares

Toda adquisición se basa en los estándares, es decir la arquitectura debe estar establecida por el Comité de Gestión de Seguridad de la información. Esta arquitectura tiene una permanencia mínima de dos a cinco años.

9.5.7. Capacidades

Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo de la Unidad. Para la adquisición de Hardware se tendrá en cuenta lo siguiente:

a) El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares de la Institución.
b) Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en el país.
c) La marca de los equipos o componentes deberán de contar con presencia y permanencia demostrada en el mercado nacional, así como con asistencia técnica y de repuestos local. Tratándose de microcomputadores, a fin de mantener actualizada la arquitectura informática de la Institución, el Comité de Gestión de Seguridad de

la información emitirá periódicamente las especificaciones técnicas mínimas para su adquisición.

d) Los dispositivos de almacenamiento, así como las interfaces de entrada y salida deberán estar acordes con la tecnología vigente, tanto en velocidad de transferencia de datos, como en procesamiento.
e) Las impresoras deberán apegarse a los estándares de Hardware y Software vigentes en el mercado y en La Institución, corroborando que los suministros (tóner, tintas, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
f) Conjuntamente con los equipos, se deberá adquirir el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
g) Los equipos adquiridos deben contar con asistencia técnica durante la instalación de los mismos.
h) En lo que se refiere a los servidores, equipos de comunicaciones, concentradores, firewalls, switches y otros equipos que se justifiquen por ser de operación crítica y/o de alto costo, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de repuestos al vencer su período de garantía.
i) En lo que se refiere a los computadores personales, al vencer su garantía por adquisición, deberán de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de repuestos.
j) Todo proyecto de adquisición de bienes de tecnología, debe sujetarse al análisis, aprobación y autorización del el Comité de Gestión de Seguridad de la información.

9.5.8. Software

En la adquisición de equipo de cómputo se deberá incluir el software vigente preinstalado con su licencia correspondiente. Para la adquisición de software base y utilitarios, el Comité de Gestión de Seguridad de la información dará a conocer periódicamente las tendencias con tecnología de vigente, siendo la principal lista de productos autorizados la siguiente:

Sistemas Operativos

- MS-Windows.
- Linux.

Base de Datos

- MS-SQL. MYSQL.
- Oracle.
- PostgreSQL.

Lenguajes y herramientas de Programación
- PHP
- Laravel
- Java
- Ruby on Rails

Suite de Oficina
- Microsoft Office
- Open Office

Programas Antivirus
- Eset Endpoint Antivirus

Gestión de Proyectos
- MS Project.

Correo Electrónico
- Outlook Express.
- Gmail.

Sistema de Control de Versiones
- Microsoft Team Foundation Servar.
- Tortoise SVN.

Herramientas de Modelado
- StarUML.
- Bizagi.
- MS Visio.

Diseño
- Adobe Creative Suite.
- CorelDRAW.

Utilitarios
- PDF Creator.
- 7zip. CCleaner. DiskCleaner. Filezilla. Notepad++. Adobe Reader.

- VLC media player.
- Navegadores de Internet Explorer. Google Chrome. Mozilla Firefox.

9.5.9. Requerimiento de Seguridad de los Sistemas

a) Se tendrá un servidor especialmente dedicado para el desarrollo de los sistemas.
b) Se tendrá un servidor especialmente dedicado para la prueba de los sistemas.
c) Se tendrá un servidor especialmente dedicado para la integración de los sistemas.
d) No se realizará ningún desarrollo sobre los servidores de producción.
e) Una vez que el sistema entre en producción, se deberá contar con uno de pruebas/manteniendo, donde se llevarán a cabo las adecuaciones y pruebas necesarias antes de pasarlas a producción.

9.5.10. Seguridad en los Sistemas de Aplicaciones

a) Las aplicaciones deberán residir en los servidores de la Institución o en los equipos que se determine que cuentan con las características técnicas suficientes para soportar la aplicación.
b) Únicamente el personal autorizado por la Unidad de Sistemas e Información tendrá acceso a la administración del sistema operativo del equipo donde reside el sistema.
c) Será responsabilidad del Equipo Funcional de Tecnologías de la Información el hardware y sistema operativo del servidor donde reside la aplicación.

9.5.11. Seguridad en el Desarrollo y procedimiento de soporte

a) El desarrollo de sistemas se debe realizar en ambientes estrictamente controlados y diferentes a los de producción, la Unidad de Sistemas e Información es responsable de brindar seguridad y el ambiente para un adecuado desarrollo.
b) Los programas fuentes de las aplicaciones de la DIRIS LIMA CENTRO deberán estar adecuadamente resguardados y solo deben ser accesible por el personal autorizado.
c) Se definirá un directorio explícito durante para el desarrollo y mantenimiento de los sistemas y no afectar el ambiente de producción.
d) El desarrollo de sistemas no se deberá realizar en el servidor de producción.

9.5.12. Control de acceso al Código Fuente de los Sistemas Desarrollados

a) Se debe restringir y controlar el acceso al código fuente de las aplicaciones informáticas o programas.
b) Se debe contar con un responsable del acceso al código fuente de los sistemas desarrollados, quien deberá implementar un registro de uso, si es que el código es requerido.

9.5.13. Uso de Controles Criptográficos

Se debe implementar el uso de controles para cifrar la información y protege la confidencialidad, autenticidad e integridad de la misma cuando sea requerido, y de acuerdo a nivel de exposición de riesgo.

9.5.14. Gestión de vulnerabilidad técnica

a) La Unidad de Sistemas e Información debe programar la realización de pruebas de comprobación técnica a cargo de especialista externos para verificar que se han implementado correctamente los controles de seguridad definidos para los desarrollos informáticos.
b) Identificadas las vulnerabilidades técnicas, se deben determinar los riesgos asociados e implementar los controles necesarios para mitigarlos. Las aplicaciones informáticas críticas y en alto riesgo deben ser tratados a tiempo.

9.6. Políticas de Seguridad Perimetral

La seguridad perimetral es uno de los métodos posibles de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y diferentes niveles. Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

El Equipo Funcional de Tecnología de la Información se encargará de vigilar y monitorear el funcionamiento de los servicios críticos del LA DIRIS LIMA CENTRO. Se encargará de prevenir ataques o delitos informáticos que se puedan presentar en la red y que violen la integridad de la información de los usuarios, de las Unidades y Oficinas Orgánicas

Los Administradores de Red implementarán soluciones lógicas y físicas que garanticen la protección de la información de las compañías de posibles ataques internos o externos.

a) Rechazar conexiones a servicios comprometidos
b) Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
c) Proporcionar un único punto de interconexión con el exterior.

d) Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red interna).
e) Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde internet.
f) Auditar el tráfico entre el exterior y el interior.
g) Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

9.6.1. Firewall

a) La solución de seguridad perimetral debe ser controlada con un Firewall por Hardware (físico) que se encarga de controlar puertos y conexiones, es decir, de permitir el paso y el flujo de datos entre los puertos, ya sean clientes o servidores.
b) Este equipo deberá estar cubierto con un sistema de alta disponibilidad que permita la continuidad de los servicios en caso de fallo.
c) Los Administradores de Red establecerán las reglas en el Firewall necesarias bloquear, permitir o ignorar el flujo de datos entrante y saliente de la Red.
d) El firewall debe bloquear las "conexiones extrañas" y no dejarlas pasar para que no causen problemas.
e) El firewall debe controlar los ataques de "Denegación de Servicio" y controlar también los números de conexiones que se están produciendo, y en cuanto detectan que se establecen más de las normales desde un mismo punto bloquearlas y mantener el servicio a salvo.
f) Controlar las aplicaciones que acceden a Internet para impedir que programas a los que no hemos permitido explícitamente acceso a Internet, puedan enviar información interna al exterior (tipo troyanos).

9.6.2. Sistemas de Detección de Intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés intrusión Detection System) es una aplicación usada para detectar accesos no autorizados a un computador/servidor o a una red. Estos accesos pueden ser ataques realizados por usuarios malintencionados con conocimientos de seguridad o a través de herramientas automáticas. Los Administradores de Red implementarán soluciones lógicas y físicas que impidan el acceso no autorizado a los equipos de La Institución:

a) Detección de ataques en el momento que están ocurriendo o poco después.
b) Automatización de la búsqueda de nuevos patrones de ataque, con herramientas estadísticas de búsqueda y al análisis de tráfico anómalo.

c) Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos.
d) Auditoría de configuraciones y vulnerabilidades de los sistemas de IDS.
e) Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs.
f) Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos u otros, existe la posibilidad de que se esté en presencia de una intrusión. Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto.
g) Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración del Firewall.
h) La Red de La Institución sólo podrá acceder a los parámetros que el Firewall tenga permitido o posibilite mediante su configuración.

9.6.3. Conectividad a Internet

a) La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de la Institución tienen las mismas responsabilidades en cuanto al uso del Internet.
b) El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.
c) Los usuarios son responsables del uso ético, legal y profesional sobre el correcto acceso a Internet.
d) Todos los usuarios de Internet se comprometen a utilizarlo exclusivamente para funciones concernientes a la Institución y en caso de recibir información ajena a la misma eliminarla inmediatamente.
e) Todos los usuarios de Internet serán sujetos de ser auditados sin previo aviso.
f) La Unidad de Sistemas e información se reserva el derecho de utilizar software o hardware que permita la identificación en línea y bloqueo del acceso a sitios específicos de Internet.
g) Queda prohibido el acceso a sitios de Internet que contengan material con contenido explícito o cualquier otro material que se considere inapropiado u ofensivo en el lugar de trabajo.
h) No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador o con otras herramientas de Internet conectándose con un módem.
i) Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con las tareas y actividades del trabajo desempeñado.
j) Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

Tipo de Documento	Numeración	Siglas de la Institución	Año calendario de Aprobación	Sigla del Órgano que genera el DN
DIRECTIVA ADMINISTRATIVA	001	DIRIS LC	2021	OTI-DA DIRIS-LC V01

k) No se permite bajar archivos de música, emisión continua (radio, por ejemplo), correo basura (cadenas, chistes, etcétera), barras de navegación, juegos y cualquier otro tipo de información que no esté relacionada con la Comisión o con las funciones propias de la plaza que se tiene a cargo.

9. RESPONSABILIDADES

9.1.1. Responsabilidad de Seguridad de los Sistemas de Información

Es de carácter obligatorio para todo el personal (Fijo, Contratado), la notificación inmediata de algún problema o violación de la seguridad, del cual tuviese conocimiento; esta notificación deberá realizarse por escrito vía correo electrónico a la Unidad de Sistemas e Información o a la Alta Dirección, quienes están en la obligación de realizar las gestiones pertinentes al caso y de ser cierta la sospecha tomar las medidas adecuadas para solucionar el incidente.

Es responsabilidad de todo servidor que maneje datos o información a través de accesos debidamente autorizados, el cumplimiento de las políticas de control de acceso, puesto que estas descansan en el establecimiento de responsabilidades donde se incurra en alguna violación en materia de seguridad acarreando sanciones a quien las haya causado, puesto que esto ocasionaría perjuicios económicos a la Institución de diversa consideración. Es por ello que las personas relacionadas de cualquier forma con los procesos tecnológicos deben ser conscientes y asumir que la seguridad es asunto de todos y, por lo tanto, se debe conocer y respetar las Políticas de Seguridad.

Está fundamentado como una exigencia que el personal de la institución conozca sus responsabilidades, sanciones y medidas a tomar al momento de incurrir en alguna violación o falta que se encuentre descrita en las Políticas de Seguridad firmado por el servidor o quien corresponda. Por esta razón, se entenderá que sólo una adecuada política de seguridad tecnológica apoyará la concientización para obtener la colaboración de los servidores, haciéndoles conscientes de los riesgos y de la importancia del cumplimiento de las normas.

9.1.2. Legalidad y Seguridad de Software

Todos los productos de Software que se utilicen deberán contar con su factura y licencia de uso respectiva, por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento. La Oficina de Tecnologías de la Información promoverá y propiciará que la

adquisición de software de dominio público provenga de sitios oficiales y seguros.

9.1.3. Derechos de Propiedad Intelectual

Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de software y demás fuentes que violen la ley de derechos de autor, para tal efecto todos los usuarios deberán firmar un documento donde se comprometan, bajo su responsabilidad, a no usar programas de software que violen la ley de derechos de autor. Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la Institución bajo ninguna circunstancia sin la autorización escrita del Equipo Funcional de Tecnología de la Información.

a) No se tolerará que un servidor realice copias no autorizadas de los programas informáticos de la Institución.
b) No se tolerará que un servidor cargue o descargue programas informáticos no autorizados de Internet, incluidos entre otros la descarga de programas informáticos que utilicen sistemas peer-to-peer (P2P - Ej. Kazaa. Ares. etc) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.
c) No se tolerará que un servidor realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o no posee los derechos de distribución del mismo.
d) Si se descubre que un servidor ha copiado programas informáticos de forma ilegal para dárselos a un tercero, también podrá ser sancionado.
e) Si un usuario requiere utilizar programas informáticos autorizados por las Institución de manera remota, debe consultar con los Administradores de Red para asegurarse de que ese uso esté permitido por la licencia de autor.
f) El personal encargado de soporte de Tecnología revisará las computadoras constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si la Institución posee licencias para cada una de las copias de los programas informáticos instalados.
g) Si se encuentran copias sin licencias, estas serán eliminadas y de ser posible, reemplazadas por copias con licencia o software libre que realice funciones similares o equivalentes.
h) La Institución autoriza el uso de programas informáticos de diversas Instituciones externas. La Institución no es dueña de estos programas informáticos o la documentación vinculada con ellos y a menos que cuente con la autorización del creador de los programas informáticos, no tiene derecho a reproducirlos excepto con fines de respaldo.
i) Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a

sanciones civiles y penales, incluidas multas y prisión. No se permite la duplicación ilegal de programas informáticos.

Los servidores que realicen, adquieran o utilicen copias no autorizadas de programas informáticos estarán sujetos a sanciones disciplinarias internas de acuerdo a las circunstancias. Dichas sanciones pueden incluir suspensiones y despidos justificados.

9.1.4. Faltas a la Política

La seguridad de la información en todos los ámbitos, debe ser considerada como un ítem dentro de la evaluación mensual de desempeño del personal.

El incumplimiento de las obligaciones y prohibiciones mencionadas en este documento y otros documentos complementarios, facultan a la DIRIS LIMA CENTRO a aplicar medidas disciplinarias de acuerdo a sus reglamentos.

10. ANEXO

GLOSARIO

1. **Backup:**
   Copia de Respaldo o Seguridad, acción de copiar archivos o datos de forma que estén disponibles en caso se produzca un fallo o la pérdida de la data original.

2. **Computador:**
   Es una máquina basada en la tecnología microelectrónica que, a través de sus diversos componentes, tanto físicos como lógicos (básicamente procesador, memoria y dispositivos de entrada/salida), permite el procesamiento de datos para obtener información.

3. **Contraseña:**
   Conjunto de caracteres que permite el acceso de un usuario a un recurso informático (password).

4. **Correo electrónico:**
   Es un servicio en el que se puede enviar y recibir mensajes de manera instantánea a través de Internet, que pueden incluir archivos adjuntos (imágenes, archivos etc.).

Tipo de Documento	Numeración	Siglas de la Institución	Año calendario de Aprobación	Sigla del Órgano que genera el DN
DIRECTIVA ADMINISTRATIVA	001	DIRIS LC	2021	OTI-DA DIRIS-LC V01

5. **Data Center:**
Se denomina centro de procesamiento de datos (CPD) a aquella ubicación donde se concentran los recursos de Tecnología de Información necesarios para el procesamiento de la información de la DIRIS LIMA CENTRO.

6. **DBA:**
Administrador de base de Datos, es el profesional que administra las tecnologías de la información y la comunicación, siendo responsable de los aspectos totales de la base de datos (aspecto técnico, tecnológico, científicos etc.)

7. **Firewall:**
Es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas externas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas, protocolos de seguridad y otros criterios.

8. **Firma digital:**
Es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma se puede garantizar la integridad del documento o mensaje y la identidad del remitente.

9. **Hacker:**
Es aquella persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.

10. **Hardware:**
Se refiere a todas las partes físicas de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

11. **Información:**
Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Tipo de Documento	Numeración	Siglas de la Institución	Año calendario de Aprobación	Sigla del Órgano que genera el DN
DIRECTIVA ADMINISTRATIVA	001	DIRIS LC	2021	OTI-DA DIRIS-LC V01

12. **Internet:**
Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación.

13. **LAN:**
Son las siglas de Local Área Network, Red de área local. Es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio o un conjunto de edificios).

14. **Login:**
Cuenta de usuario para el acceso a los recursos en la red Institucional.

15. **Macro:**
Son una serie de instrucciones que se almacenan para que se puedan ejecutar de manera secuencial mediante una sola llamada u orden de ejecución. Con frecuencia se los utilizan en los documentos de MS EXCEL, MS WORD y otros de la suite de Microsoft Office.

16. **Malware:**
También llamado badware, código maligno, software malicioso o software malintencionado, es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. El término malware es muy utilizado por profesionales de la informática para referirse a una variedad de softwares hostiles, intrusivos o molestos. El término virus informático suele aplicarse de forma incorrecta para referirse a todos los tipos de malware, incluidos los virus verdaderos.

17. **Memoria USB:**
Es un tipo de dispositivo de almacenamiento de datos que utiliza memoria flash para guardar datos e información. Se le denomina también como memoria externa.

18. **Red inalámbrica:**
Designa a la conexión de nodos que se da por medio de ondas electromagnéticas, sin necesidad de una red cableada. La transmisión y la recepción se realizan a través de puertos.

19. **Red privada virtual o VPN:**
Es una tecnología que permite una extensión segura de la red local (u\N) sobre una red pública o no controlada como Internet. Permite que la computadora en

la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos.

20. **Registro:**
Es un conjunto de campos que contienen los datos que pertenecen a una misma repetición de entidad. Se le asigna automáticamente un número consecutivo (número de registro) que en ocasiones es usado como índice, aunque lo normal y práctico es asignarle a cada registro un campo clave para su búsqueda.

21. **Responsable de Activos:**
Personal del área administrativa – Unidad de Control Patrimonial de la Institución, que velará por la seguridad y correcto funcionamiento de los activos informáticos, así como de la información procesada en éstos, dentro de sus respectivas áreas. Esta persona debe mantener el inventario físico al día, velar por que todos los activos tengan sus respectivas pólizas de seguros bajo los parámetros entregados por la Alta Dirección.

22. **Router:**
Es un dispositivo que proporciona conectividad a nivel de red. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes.

23. **Servidor:**
Son modelos de computadora diseñados para hospedar un conjunto de aplicaciones que tiene gran demanda dentro de una red. En esta configuración cliente- servidor, uno o más equipos, lo mismo una computadora que una aplicación informática, comparten información entre ellos de forma que uno actúa como host de los otros.

24. **Sistema de información:**
Todo aquel programa o software informático que se ha confeccionado para brindar un servicio de manejo de información, la misma que puede haber sido creada por personal del Ministerio Público o se haya adquirido.

25. **Sistema Operativo:**
Un sistema operativo es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes.

26. Software:
Estos son los programas informáticos que hacen posible la realización de tareas específicas dentro de un computador. Por ejemplo, Word, Excel, PowerPoint, los navegadores web, los juegos, los sistemas operativos, etc.

27. Solución Antivirus:
Recurso informático empleado para solucionar problemas causados por virus informáticos. Su finalidad es prevenir los virus informáticos, así como curar los ya existentes en un sistema. Estos programas deben actualizar ser periódicamente.

28. Spyware:
Es un programa espía que recopila información de un equipo informático y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del equipo informático.

29. Teléfono inteligente (Smartphone):
Es un teléfono móvil construido sobre una plataforma informática móvil, con una mayor capacidad de almacenar datos y realizar actividades semejantes a una minicomputadora y con una mejor conectividad y capacidades que un teléfono móvil convencional.

30. Troyano:
Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

31. USB:
Es el puerto que permite funcionar como dispositivo que facilita la conexión de periféricos y accesorios a un ordenador, permitiendo el fácil intercambio de datos y la ejecución de operaciones.

32. Usuarios:
Cualquier persona (servidor o no) que haga uso de los servicios de las tecnologías de Información proporcionada por la institución tales como equipos de cómputo, sistemas de información, redes de telemática, etc.

Tipo de Documento	Numeración	Siglas de la Institución	Año calendario de Aprobación	Sigla del Órgano que genera el DN
DIRECTIVA ADMINISTRATIVA	001	DIRIS LC	2021	OTI-DA DIRIS-LC V01

33. Videoconferencia:

Es el sistema que permite la comunicación bidireccional simultánea (en tiempo real), persona a persona o grupo a grupo, en la cual se transmite voz, video y, opcionalmente, datos, textos y/o gráficos.

34. Virus Informático:

Programa ejecutable o pieza de código con habilidad de ejecutarse y reproducirse, regularmente escondido en documentos electrónicos que causan problemas al ocupar espacio de almacenamiento, así como destrucción de datos y reducción del desempeño de un equipo de cómputo.

35. Vulnerabilidad:

Son puntos débiles del software que permiten que un atacante comprometa la integridad, disponibilidad o confidencialidad del mismo. Algunas de las vulnerabilidades más severas permiten que los atacantes ejecuten código arbitrario, denominadas vulnerabilidades de seguridad en un sistema comprometido.