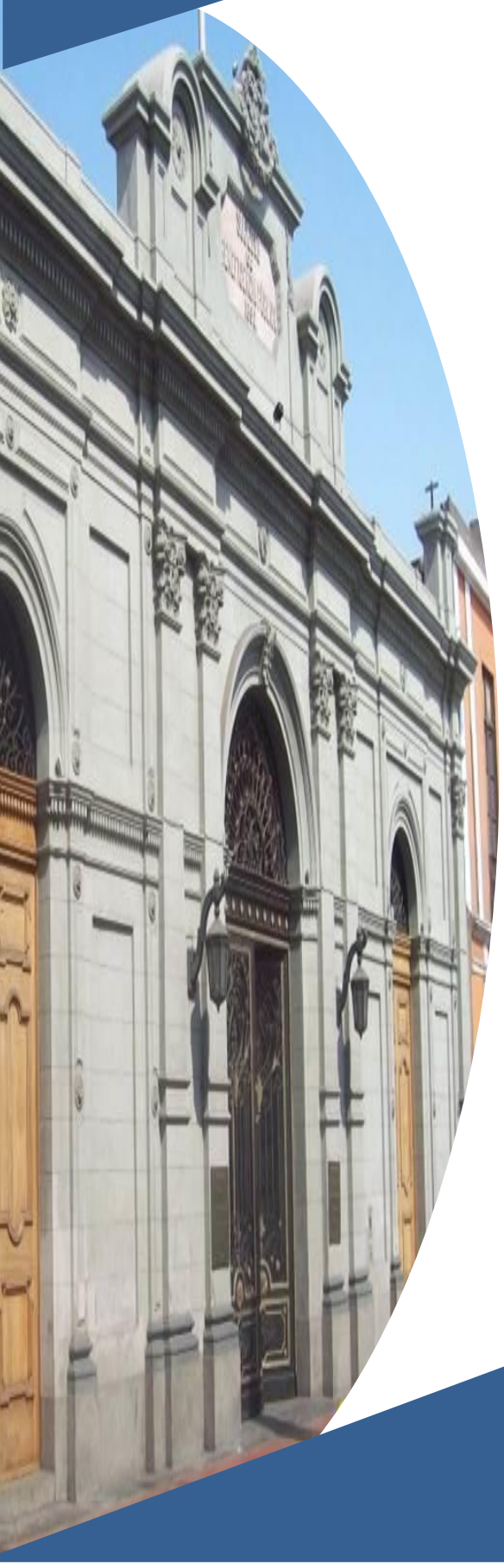

Beneficencia de Lima
—1834

POLÍTICA DE SEGURIDAD INFORMÁTICA

Beneficencia
de Lima
—1834

ÍNDICE

Beneficencia
de Lima
—1834

1. PRESENTACIÓN

La Sociedad de Beneficencia de Lima Metropolitana, no se constituye como una institución pública, se rigen por lo establecido en el Decreto Legislativo N° 1411 y para su adecuado control, por las normas de los sistemas administrativos de defensa judicial del Estado y control; así como por las normas que regulan los bienes estatales en lo que respecta a la disposición de bienes inmuebles de las Sociedades de Beneficencia; y de manera subsidiaria por las normas del Código Civil y la Ley General de Sociedades.

El Decreto Legislativo N° 1411 faculta al Ministerio de la Mujer y Poblaciones Vulnerables para emitir los lineamientos necesarios para la implementación de buenas prácticas de gestión, seguridad de la información, seguridad informática, entre otras normas.

De acuerdo a ello, la Sociedad de Beneficencia de Lima Metropolitana, debe asegurar la confidencialidad, disponibilidad e integridad de la información con la implementación de medidas y controles de seguridad informática.

La Seguridad Informática permitirá que los activos de información que se procesan dentro de la infraestructura tecnológica de la Sociedad de Beneficencia de Lima Metropolitana se encuentren protegidos con un nivel mínimo de riesgo a la seguridad de la información digital.

2. BASE LEGAL:

a) La Constitución Política del Perú.
b) Decreto Legislativo N° 1411, que regula la Naturaleza Jurídica, Funciones, Estructura Orgánica y Otras Actividades de las Sociedades de Beneficencia y sus modificaciones.
c) Ley N° 29733 - Ley de Protección de Datos Personales y modificatorias.
d) Ley N° 30096 - Ley de Delitos Informáticos.
e) Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley de Protección de Datos Personales.
f) Resolución Ministerial N° 185-2021-MIMP, Aprueba los "Lineamientos para la Implementación de Buenas Prácticas de Gestión de las Sociedades de Beneficencia".
g) Resolución de Gerencia General N° 013-2023-GG/SBLM, Aprueba la actualización del Manual Estructural, Orgánico y Funcional de la Sociedad de Beneficencia de Lima Metropolitana.

3. ALCANCE:

La Política de Seguridad Informática, es de cumplimiento obligatorio de todos los colaboradores de la SBLM, bajo cualquier modalidad contractual.

4. PRINCIPIOS:

4.1. Confidencialidad: Es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Es un principio fundamental de la seguridad de la

información que garantiza el necesario nivel de secreto de la información y de su tratamiento, para prevenir su divulgación no autorizada cuando está almacenada o en tránsito.

4.2. Integridad: Es la capacidad para proteger la exactitud y corrección de los datos, es decir, la capacidad para evitar que los datos sean alterados, modificados o corrompidos de manera intencional por actores no autorizados, o no intencional, es decir, por un error de los usuarios autorizados o cualquier otro incidente de origen no malicioso.

4.3. Disponibilidad: Es la capacidad de acceder a la información cuando se necesite, sin interrupciones y sin excesivas complicaciones. Si la disponibilidad de la información se ve comprometida, habrá tareas que no se podrán realizar y, en determinados casos, incluso podría suponer la interrupción completa de la actividad o el servicio.

5. DEFINICIONES

5.1. Auditoria: Proceso por el que se lleva a cabo una inspección y examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento con la política establecida y procedimientos operativos, y para recomendar cualquier cambio que se estime necesario.

5.2. Bases de Datos: Es un conjunto de datos interrelacionados. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápido.

5.3. Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, instituciones o procesos autorizados.

5.4. Control de Acceso: Técnica usada para definir el uso de programas o limitar la obtención y almacenamiento de datos a una memoria y/o persona; Es una característica o técnica en un sistema de comunicaciones que permitirá o negará el uso de algunos componentes o de algunas de sus funciones.

5.5. Contraseña o Clave: Conjunto finito de caracteres limitados que forman una palabra secreta que sirve a uno o más usuarios para acceder a un determinado recurso. Las claves suelen tener limitaciones en sus caracteres (no aceptan algunos), así como de su longitud.

5.6. Desarrolladores de Sistemas: Colaboradores quienes "en representación del usuario" seleccionan, desarrollan y dan mantenimiento a los sistemas automatizados.

5.7. Dueño (Propietario) del Sistema: Colaborador responsable por la definición y aceptación de los requerimientos para el desarrollo y mantenimiento de los sistemas automatizados y con autoridad sobre su uso.

5.8. Estándar: Patrón uniforme o muy generalizado de un procedimiento establecido.

5.9. Colaboradores: Personal de la SBLM, indistintamente del régimen de contratación.

5.10. Custodio de la Información: Es el responsable de resguardar los activos de información que custodia, así como los medios en los cuales dichos activos residen o se soportan, aplicando controles de seguridad razonables con la finalidad de minimizar los riesgos.

5.11. Gerente del Proyecto: Colaborador responsable de coordinar las actividades administrativas relacionadas con el proyecto y su ciclo de vida (análisis, pruebas, capacitación, implementación, y otros).

5.12. Líder técnico: Analista de alto nivel con amplia trayectoria en análisis, responsable de brindar apoyo técnico al gerente del proyecto y de coordinar las diferentes instancias ante la SBLM en el desarrollo de un proyecto.

5.13. Mejores Prácticas: Corresponde a un modelo completamente definido, cuyos buenos resultados operacionales están comprobados y que está disponible para ser utilizada.

5.14. Política: Es una actividad orientada en forma ideológica a la toma de decisiones de un grupo para alcanzar ciertos objetivos.

5.15. Política de Seguridad Informática: Una política de seguridad informática es una forma de comunicarse con los usuarios. Las políticas de seguridad informática establecen el canal formal de actuación del colaborador, en relación con los recursos y servicios informáticos importantes de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de lo que deseamos lograr con la protección y el porqué de ello. Cada política de seguridad informática es consciente y vigilante del colaborador por el uso y limitaciones de los recursos y servicios informáticos críticos de la SBLM.

5.16. Procedimiento: Sucesión cronológica de operaciones concatenadas entre sí, que se constituyen en una unidad de función para la realización de una actividad o tarea específica dentro de un ámbito predeterminado de aplicación.

5.17. Propietario de la Información: Es el responsable de clasificar el nivel de confidencialidad de la información y de definir los usuarios que podrían acceder a la información de acuerdo a sus funciones y competencias.

5.18. Red LAN: Red de Área Local (Local Área Network).

5.19. Red WAN: Red de Área Ancha (Wide Área Network).

5.20. Sistemas críticos: Sistemas fundamentales para las operaciones de la SBLM, para el cumplimiento de su misión y visión.

5.21. Software de aplicación: Es aquel destinado a satisfacer las necesidades funcionales de los colaboradores que puede ser desarrollado tanto interna como externamente.

5.22. Usuario: Es aquel colaborador que tiene relación directa con la institución y tiene asignado un activo informático.

5.23. Computadora personal: Computador u ordenador asignado al colaborador de la Institución, conforme a los procedimientos previstos. Comprende el CPU (incluye teclado y mouse) y Monitor.

6. CONSIDERACIONES GENERALES

6.1. Toda política de seguridad informática deberá seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes: crecimiento de la planta de personal, cambio en la infraestructura computacional, desarrollo de nuevos servicios, cambios vertiginosos de la tecnología, entre otros.

6.2. Se prohíbe totalmente la publicación de datos sensibles de los colaboradores de la SBLM, así como de toma fotográfica que atenten contra la reputación, imagen y buen nombre de las personas.

6.3. El uso inadecuado de los recursos tecnológicos o incumplimiento a alguna de las presentes políticas dará lugar en primera instancia a una amonestación por correo por parte de la Gerencia de Tecnologías de Información y Comunicaciones, de persistir y/o reincidir, se suspenderán los servicios a los usuarios que incumplan, debiéndose comunicar a la Subgerencia de Recursos Humanos para las acciones administrativas correspondientes.

Beneficencia
de Lima
—1834

7. POLÍTICA DE SEGURIDAD INFORMÁTICA

La Gerencia de Tecnologías de la Información y Comunicaciones, se compromete a proteger la información institucional que se genera, circula, procesa y almacena por medios digitales.

La Subgerencia de Seguridad e Infraestructura Informática, liderará la revisión, cumplimiento y mejoramiento continuo de la seguridad informática, para lo cual deberá generar la documentación necesaria como procedimientos, manuales, instructivos y demás elementos que sean necesarios para tal fin.

Las políticas relacionadas a la Seguridad de la Información como es el presente documento, deberán ser difundidas a través de medios digitales a todos los colaboradores involucrados en su definición.

8. APLICACIÓN DE SEGURIDAD INFORMÁTICA

8.1. RESPONSABILIDADES

- ✓ **Gerencia de Tecnologías de Información y Comunicaciones:** Velar por el cumplimiento de la presente política, garantizando los niveles de seguridad adecuados para el uso de los dispositivos digitales institucionales.
- ✓ **Subgerencia de Seguridad e Infraestructura Informática:** Designar el personal idóneo para que establezca y configure los dispositivos, redes de datos, elementos de seguridad, estaciones de trabajo y demás elementos que hagan parte de la red de datos y servicios digitales de la SBLM, acogiendo los lineamientos de seguridad definidos en la presente política.
- ✓ **Colaborador:** Hacer uso responsable de los equipos de tecnología informática acogiendo los lineamientos establecidos por la SBLM.

8.2. GENERALIDADES

- ✓ Los usuarios de los servicios tecnológicos se regirán por los lineamientos técnicos establecidos por la Gerencia de Tecnologías de Información y Comunicaciones.
- ✓ Todo colaborador es responsable de reportar inmediatamente las anormalidades e incidentes de seguridad informática a la Subgerencia de Seguridad e Infraestructura Informática.
- ✓ Las modificaciones a los datos e información de los sistemas en producción deben estar estrictamente restringidas a las transacciones y procesos expresamente diseñados para tal fin.
- ✓ Todos los equipos de tecnología informática (computadoras, estaciones gráficas, servidores y equipamiento accesorio, dispositivos móviles, tabletas, smartphone), que esté o sea conectado a la Red de la SBLM o que use la red de datos de la organización, deberá sujetarse a las normas y parámetros de instalación y configuración que emita la Gerencia de Tecnologías de Información y Comunicaciones.
- ✓ La Gerencia de Tecnologías de Información y Comunicaciones, deberá tener un registro en donde se asocie el usuario con la estación de trabajo, la dirección IP y el perfil de navegación asignado.
- ✓ La Subgerencia de Soporte y Desarrollo Informático deberá tener un registro de todos los equipos de propiedad de la SBLM, debiendo contener el nombre del colaborador que tiene a cargo el equipo o recurso tecnológico, actualizando el inventario permanentemente.

8.3. CONTROL DE ACCESO

- ✓ Cada usuario debe tener una identificación única e intransferible dentro de cada sistema. La combinación de usuario y clave deben ser únicos.
- ✓ Los nombres de usuario y claves son personales e intransferibles, y solamente deben ser utilizados por el colaborador al que le fueron asignados. Está totalmente prohibido que un colaborador autorice el uso de clave a terceros o que preste sus credenciales de acceso.
- ✓ Todo colaborador será responsable de las actividades y transacciones que sean realizadas con su usuario y clave de carácter confidencial.
- ✓ Los derechos de acceso de los usuarios a las transacciones específicas de cada uno de los sistemas de información deben estar formalmente autorizados por la Gerencia de Tecnologías de Información y Comunicaciones a través de su Gerencia y/o área respectiva.
- ✓ Los derechos de acceso deben ser asignados de tal forma que no interfieran con las actividades o datos privados de otros usuarios.
- ✓ Al asignarse por primera vez el password a un colaborador, ésta deberá ser cambiada por el citado colaborador en forma inmediata:
  - Las claves de usuario deben ser alfanuméricas, contener caracteres especiales y una longitud no menor a 8 (ocho) caracteres sin utilizar espacios en blanco.
  - Deben contener tanto caracteres alfabéticos como numéricos.
  - No deben estar basados en palabras de un diccionario, para no ser fácilmente descifrados. No deben revelarse bajo ninguna circunstancia.
  - El nombre de usuario y la clave deben ser diferentes entre sí.
  - No se deben utilizar claves con información fácilmente identificable como, fecha de cumpleaños, nombres de familiares y apellidos, números de identificación, y/o demás información personal evidente.
  - Las claves no deberán de repetirse, las mismas que deberán ser cambiadas como mínimo cada seis meses.

- ✓ Se debe mantener en un sobre sellado y lacrado bajo la responsabilidad de la Subgerencia de Seguridad e Infraestructura Informática: el usuario Administrador de la Red, Administrador de Base Datos, Administrador de Sistemas de Información u otros, las mismas que deberán de aperturarse sólo en casos de emergencia. En caso de requerir su uso debe quedar debidamente registrado. La clave debe ser cambiada periódicamente mínimo dos veces al año.
- ✓ Debe mantenerse activo el cambio automático de clave, según las políticas establecidas en el directorio activo; es responsabilidad de todos los colaboradores cambiar su clave.
- ✓ La Subgerencia de Seguridad e Infraestructura Informática es responsable de dejar deshabilitados los derechos de acceso de aquellos colaboradores que presenten novedades de personal (descanso médico, permisos y otros), basándose en la información reportadas por la Subgerencia de Recursos Humanos. En caso de requerir el acceso a la cuenta del usuario, el Gerente autorizará si así lo requiere los nuevos accesos del personal de remplazo de los privilegios que fueron suspendidos temporalmente hasta el regreso del titular.
- ✓ El tiempo de acceso a los sistemas debe permitirse dentro de un horario particular de acuerdo con las necesidades de la oficina, en caso de requerirse las Gerencias deberán estar informadas de los horarios extendidos.

- ✓ Las cuentas de usuario que permanezcan inactivos por más de 30 (treinta) días deben quedar deshabilitados. Podrán ser activados nuevamente mediante solicitud formal de la Gerencia del usuario hacia el Gerente de Tecnologías de la Información y Comunicaciones; quedando totalmente prohibido el uso de la cuenta por otro colaborador, salvo autorización expresa de su Gerencia.
- ✓ Los privilegios especiales del sistema operativo o software utilitario, que permitan examinar el contenido de los archivos de otros usuarios, deben restringirse únicamente a personal de la Subgerencia de Seguridad e Infraestructura Informática.
- ✓ No se deben dejar nombres de usuario y claves escritos en lugares donde puedan ser vistos o tomados por terceros (por ejemplo, en la carpeta del escritorio, pantalla del equipo, bajo el teclado... etc.)
- ✓ Los colaboradores no deben dejar desatendidas las estaciones de trabajo. Todo colaborador es responsable de desactivar las aplicaciones (cerrarlas) de ser necesario, cada vez que se ausente de su puesto de trabajo, y dejarla bloqueada con contraseña.

8.4. INTERNET

- ✓ El acceso a Internet e Intranet, es una herramienta de trabajo que provee la Institución a sus colaboradores, por lo tanto, es responsabilidad de cada colaborador, utilizar prudente y apropiadamente este servicio.
- ✓ Todo evento que se dé a través del uso de este servicio, será administrado, monitoreado y regulado por la Subgerencia de Seguridad e Infraestructura Informática el cual tendrá la potestad de realizar las acciones pertinentes en pro de la seguridad, confidencialidad, integridad y disponibilidad de los bienes informáticos y de la información de la SBLM, así mismo, reportará a la Subgerencia de Seguridad e Infraestructura Informática sobre cualquier uso indebido del servicio.
- ✓ Se prohíbe el acceso a sitios de Internet que no tengan relación alguna con los objetivos institucionales, tales como los relacionados con: sexo, racismo, apuestas, actividades criminales, drogas, juegos, y cualquier otra que se estime conveniente restringir, en relación al uso de buenas prácticas y protección de la red.
- ✓ Desde la Subgerencia de Seguridad e Infraestructura Informática se crearán y monitorearán perfiles de navegación con la finalidad de brindar a los usuarios medios de acceso y consulta a Internet.
- ✓ La asignación de perfiles de navegación será previo análisis de necesidad y autorización de la Gerencia respectiva.
- ✓ Toda información descargada de Internet debe estar relacionada con los objetivos misionales, gerenciales y/o de apoyo de la SBLM y las funciones que lleva a cabo el colaborador.
- ✓ Todos los archivos obtenidos de Internet deben ser revisados (filtrados) por el sistema de seguridad, para detección de malwares previo a ser descargados en cualquier computador, para ello debe estar instalado en todas los PC de la SBLM el EDR Corporativo.
- ✓ El tiempo de acceso a Internet no debe interferir ni distraer a los usuarios de sus funciones normales.

8.5. CORREO ELECTRÓNICO

- ✓ El Correo Electrónico, es una herramienta de trabajo que provee la SBLM a sus colaboradores, por lo tanto, es responsabilidad de cada colaborador, utilizar prudente y apropiadamente este servicio.

- ✓ Todo evento que se dé a través del uso del Correo Electrónico, será administrado, monitoreado y regulado por la Subgerencia de Seguridad e Infraestructura Informática el cual tendrá la potestad de realizar las acciones pertinentes con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de los bienes informáticos y de la información de la SBLM.
- ✓ El contenido de los mensajes creados, enviados, recibidos y almacenados debe limitarse a los propósitos Misionales y/o Operativos de la SBLM, su contenido debe ser respetuoso y no debe atentar contra la imagen ni integridad moral de sus colaboradores.
- ✓ Queda totalmente prohibido enviar mensajes de correo electrónico masivos por parte de personal no autorizado. Tales permisos quedan reservados para la Gerencia de Relaciones Institucionales, Subgerencia de Recursos Humanos, Oficina de Compliance y Gestión de Riesgos, así como para la Gerencia de Tecnologías de la Información y Comunicaciones.
- ✓ Las cuentas de correo electrónico institucional deberán ser usadas solamente para fines laborales; no para suscripción de servicios y/o listas de correo relacionadas con temas personales.
- ✓ El tamaño de los archivos que circulan por correo electrónico o a través de los canales de comunicación, así como el espacio del buzón asignado a cada usuario para el almacenamiento de estos archivos, se hará con base a las necesidades de los usuarios mediante la definición de perfiles, así mismo, cada usuario está obligado a tener en su equipo de cómputo, un archivo de almacenamiento de correos .PST, para lo cual solicitará apoyo a la Subgerencia de Desarrollo y Soporte Informático para la capacitación correspondiente.
- ✓ La información que se haya definido como sensible por la SBLM se puede transferir por medio de correo electrónico solamente, si existe la necesidad real de transferir la información.
- ✓ Tratándose de archivos cuyo contenido sea reservado, los usuarios deberán almacenarlos en la propia computadora personal, debiendo abstenerse de copiarlos en los Directorios Grupales. Está prohibido copiar dentro de la Red de datos, archivos de entretenimiento, como videos, música, juegos, entro otros, por lo que este tipo de archivos será eliminado diariamente sin previo aviso por la Subgerencia de Seguridad e Infraestructura Informática.
- ✓ Los usuarios deben mantener activo permanentemente el correo electrónico, así como deberán conectarse como mínimo, una vez al día, para leer los mensajes, comunicados o cualquier tipo de notificación institucional, debiéndose presumir su lectura y conocimiento por el titular del correo a partir de las 24 horas del día hábil siguiente de la recepción del mensaje correspondiente, salvo excepciones debidamente justificadas.
- ✓ Los usuarios deberán ser cautelosos en la recepción de cualquier correo con remitentes y archivos adjuntos desconocidos, llámese archivos con extensión exe, com, pif, tif, entre otros, o correos con títulos sugerentes, como "I love you", entre otros. Ellos deben ser inmediatamente eliminados y notificados a la Subgerencia de Seguridad e Infraestructura Informática, con copia a Gerencia de Tecnologías de la Información y Comunicaciones.

8.6. USO DE TELÉFONOS MÓVILES

- ✓ La SBLM pone a disposición de algunos colaboradores, teléfonos móviles institucionales para facilitar el desempeño de sus labores y promueve que dichos colaboradores hagan un uso responsable de ellos.
- ✓ La Subgerencia de Soporte y Desarrollo Informático deberá contar con un listado actualizado en donde se relacione:
  - Identificación del Dispositivo Móvil (Marca, Modelo, Serial, IMEI)

- Número celular asignado
- Nombre de responsable del Dispositivo
- Listado de Software Instalado
- Ubicación Física (Gerencia)
- Detalle de configuración de las cuentas de correo configuradas en el dispositivo (Conexión con Correo Institucional) y administración y gestión remota para borrado en caso de emergencia.

✓ Los usuarios deben mantener la configuración del dispositivo y no están autorizados a desinstalar y/o instalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo; únicamente se deben aceptar y aplicar las actualizaciones.

✓ Los usuarios no deben almacenar información personal en los dispositivos móviles asignados por la SBLM.

✓ Está prohibido realizar instalación de aplicaciones no autorizadas por la Gerencia de Tecnologías de Información y Comunicaciones.

✓ Está prohibido hacer volcado de pila o reinstalación del sistema operativo por parte del usuario en el dispositivo.

8.7. SISTEMAS DE INFORMACIÓN

✓ La instalación, diseño, creación y uso de los sistemas de información se rigen por las solicitudes realizadas a través de los formatos establecidos para tal fin, y bajo los parámetros de seguridad que se establezcan en los documentos de solicitud existentes.

✓ Todos los sistemas de información, herramientas de datos (programas, bases de datos, interfaces y demás) desarrollados con los recursos de la SBLM se mantendrán como propiedad de la institución, respetando la propiedad intelectual del mismo, incluyendo sus diseños, fuentes, documentación y demás aspectos de desarrollo.

✓ Todos los sistemas de información deberán ser desarrollados y documentados de acuerdo con la metodología estándar definida por la Gerencia de Tecnologías de Información y Comunicaciones.

✓ Todo sistema de información, deberá tener asignado un administrador del sistema, responsable de las actividades de operación, manejo y cumplimiento de la seguridad establecida.

✓ La Subgerencia de Seguridad e Infraestructura Informática será responsable de mantener la operatividad del servidor y atenderá las fallas que el mismo presente tanto a nivel del sistema operativo como a nivel de hardware, Storage.

✓ La Subgerencia de Seguridad e Infraestructura Informática garantizará a los usuarios, de mantener los servicios activos, contar con los recursos de almacenamiento en forma eficiente, así como mantener un proceso adecuado del respaldo de la información.

✓ La Subgerencia de Seguridad e Infraestructura Informática será responsable de monitorear la utilización de los recursos de hardware en los servidores. Esto con el fin de proceder a la actualización del mismo en el caso de ser requerido para garantizar la continuidad de los servicios.

✓ La Gerencia de Tecnologías de Información y Comunicaciones notificará a los usuarios las ventanas de mantenimiento o la suspensión del servicio por razones de mantenimiento o por fallas ocurridas en la operatividad del mismo.

✓ Todo cambio deberá ser documentado, y de igual forma, deberá contar con una ventana de mantenimiento para su puesta en producción. Dichas ventanas de mantenimiento deben estar

debidamente documentadas indicando fecha, responsable, servidor y aplicativo afectado, además de la razón de los cambios efectuados.

- ✓ La institución deberá contar con ambientes separados para Desarrollo, Pruebas y Puesta en Producción de los Sistemas de Información. Bajo ningún motivo se podrá desarrollar aplicaciones en el ambiente de producción.

8.8. TRANSFERENCIA DE INFORMACIÓN

- ✓ La documentación, software o cualquier tipo de información de uso, no debe ser transferida a terceros sin que medie autorización de la Gerencia respectiva.
- ✓ Toda información que se genere, procese, almacene y/o transite por la red de datos de la SBLM se considera como propiedad de la SBLM.
- ✓ La información transmitida, procesada y/o almacenada, producto de las funciones del personal y que concierne a la SBLM, no podrá ser interceptada o divulgada bajo ninguna circunstancia, por ningún usuario interno de la red de la SBLM, salvo en aquellos casos que se establezcan bajo órdenes judiciales.
- ✓ Queda totalmente prohibido cargar información de la institución a nubes públicas como los son Dropbox, OneDrive, Google Drive o Servicios similares, sin previa autorización de la Gerencia de Tecnologías de la Información, quién llevará a través de la Subgerencia de Seguridad e Infraestructura Informática el monitoreo correspondiente.
- ✓ En caso de requerirse transferir información a un tercero debidamente autorizado, el dueño de la información deberá solicitar asesoría a la Subgerencia de Seguridad e Infraestructura Informática sobre el cifrado de la información y uso de llaves criptográficas.

8.9. GESTIÓN DE RECURSOS HUMANOS

- ✓ Antes de empezar a ejecutar las funciones por las cuales se adquiere vínculo con la SBLM, el personal deberá recibir una inducción, así como deberá ser capacitado en las políticas con las cuales adquiere responsabilidad de los sistemas de información con los cuales tendrá contacto, debiéndose dejar evidencia de dichas capacitaciones.
- ✓ Se deberá realizar reinducción permanente (mínimo una vez al año) en las temáticas de políticas de Seguridad de la Información y Seguridad Informática.
- ✓ Al cambiar la relación laboral de cualquier colaborador, será responsabilidad de la Subgerencia de Recursos Humanos informar a la Subgerencia de Seguridad e Infraestructura Informática las novedades de personal, quien a su vez deberá revocar y/o cambiar los derechos del usuario. El perfil local del usuario (PC de trabajo) será almacenado por un tiempo pertinente para su posterior acceso en caso de ser necesario.
- ✓ En caso de finalizar el vínculo entre el colaborador y la SBLM, se deberá hacer entrega de la información a la cual tuvo acceso; esto deberá ser informado al Subgerente del área al cual perteneció; NO se podrá realizar el cese correspondiente, hasta que no se dé visto bueno del Subgerente del área correspondiente, de haber recibido la totalidad de la información a la que haya tenido acceso y uso del propio colaborador.
- ✓ La información del colaborador que haya prestado servicios en la SBLM, deberá permanecer bajo custodia de la Subgerencia de Seguridad e Infraestructura Informática, por un periodo de 12 meses, para su posterior eliminación correspondiente.

8.10. REDES INALÁMBRICAS

- ✓ Los equipos y antenas inalámbricas única y exclusivamente deberán ser instalados por personal por la Subgerencia de Seguridad e Infraestructura Informática; además de ser el encargado de la supervisión y monitoreo.
- ✓ Los usuarios deberán evitar el mal uso de la red inalámbrica de la SBLM, como el acceso a sistemas o aplicaciones no autorizadas (Redes Sociales, reproducción de videos, juegos en línea, descarga de aplicativos) que afecten el desempeño de la red inalámbrica diseñada y destinada con fines netamente laborales, para aplicativos misionales y de apoyo y páginas corporativas de aplicaciones de la SBLM.
- ✓ Se monitoreará las páginas visitadas, y las mismas serán restringidas a través de los perfiles de navegación definidos, según se requiera previa justificación de la necesidad. En caso de hacer mal uso de los recursos o violar alguno de los lineamientos de la institución o atentar contra la Disponibilidad, Integridad o Confidencialidad de la información de la institución, la Gerencia de Tecnologías de la Información y Comunicaciones estará en la potestad de eliminar los permisos asignados e informar al Gerente de quien infrinja lo establecido.
- ✓ Se generarán informes de monitoreo de los equipos conectados a la Wifi de la institución, así como los reportes necesarios de saturación de canal páginas visitadas, top 10 de consumo en ancho de banda y páginas visitadas y demás que se requieran.
- ✓ Se encuentra terminantemente prohibido que las estaciones de trabajo se encuentren conectadas mediante la tecnología módems celulares y/o WiFi simultáneamente, mientras se encuentren conectadas a las redes de área local o cualquier otra red de comunicación interna.

8.11. COPIAS DE SEGURIDAD

- ✓ Será responsabilidad de cada usuario realizar el respaldo de su información que se encuentra en el CPU asignado. De la misma manera, cada Gerencia serán responsables de los archivos e información que sean de uso común para el desarrollo de sus actividades misionales.
- ✓ Es obligación y de responsabilidad de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma, por considerarse un activo de la SBLM, la misma que deberá preservarse; Las citadas copias deberán ser periódicas. Los usuarios deberán comunicarse con la Subgerencia de Desarrollo y Soporte Informático con el fin de establecer los medios adecuados para efectuar las copias de seguridad requeridas.
- ✓ Corresponderá a la Subgerencia de Desarrollo y Soporte Informático promover y difundir los mecanismos de respaldo para la salvaguarda de los datos, así como de los Sistemas de Información.
- ✓ La Subgerencia de Desarrollo y Soporte Informático es responsable de realizar el respaldo de la Información de los Servidores Institucionales.

8.12. REGISTRO DE ACTIVIDADES / TRANSACCIONES

- ✓ Cada sistema de información deberá contener un diaria de bitácora con información necesaria para identificar el nombre de usuario del colaborador responsable de su uso.
- ✓ El acceso a las bitácoras del sistema debe estar restringido al personal autorizado.

- ✓ Los registros de eventos sensibles contenidos en la bitácora que pueden comprometer la confidencialidad y confiabilidad de los datos, así como de sus procesos deberán estar restringidos al personal autorizado (Gerencia de TIC), los mismos que deberán ser revisados periódica y oportunamente por las Subgerencias de Desarrollo y Soporte Informático y de Seguridad e Infraestructura Informática.
- ✓ Los servidores de bases de datos institucionales, de apoyo y administrativos son de acceso controlado y confidenciales, por ello son de acceso restringido; En ese sentido, deberá quedar registrado permanentemente las diferentes copias de seguridad de las Bases de Datos que se efectúen, las mismas que deberán de informarse en forma periódica (cada 15 días) a la Gerencia de Tecnologías de la Información y Comunicaciones.
- ✓ La SBLM deberá contar con las herramientas necesarias que permitan registrar las actividades que realicen los dentro de los Sistemas de Información, Directorio activo, Servidores de archivos, navegación y transferencia de archivos.
- ✓ La Subgerencia de Seguridad e Infraestructura Informática deberá realizar revisión periódica (mínimo cada tres meses) de las actividades realizadas por los administradores de los sistemas.

8.13. SOFTWARE Y LICENCIAMIENTO

- ✓ En los equipos de la SBLM únicamente se debe tener instalado software licenciado debidamente autorizado por la Gerencia de Tecnologías de la Información y Comunicaciones.
- ✓ Es responsabilidad de la Subgerencia de Desarrollo y Soporte Informático tener un listado del Software autorizado que deberá estar instalado en los equipos de trabajo (Computadores, Portátiles, Tabletas, etc.), así como efectuar el monitoreo, a fin de que NO se instale software adicional no licenciado.
- ✓ Es responsabilidad de la Subgerencia de Desarrollo y Soporte Informático mantener actualizado el listado del licenciamiento del Sistema Operativo, Aplicaciones y demás Software debidamente autorizado a requerimiento de los usuarios de la SBLM.
- ✓ En el caso se requiera software gratuito o de uso restringido, solo podrá "descargarse" para la realización de pruebas, y su uso debe estar justificado ante la Gerencia del área, así como a la Gerencia de Tecnologías de la Información y Comunicaciones para su respectiva autorización y registro correspondiente.
- ✓ La Subgerencia de Seguridad e Infraestructura Informática realizará periódicamente el monitoreo del Software utilizado dentro de la Institución; por lo que de encontrarse Software no autorizado serán reportados a los Gerentes, así como al colaborador involucrado para tomar las medidas y acciones correctivas.

8.14. ESCRITORIO LIMPIO

- ✓ Es responsabilidad de la Subgerencia de Seguridad e Infraestructura Informática para la implementación de carpetas virtualizadas para todos los usuarios, a fin de que los mismos puedan almacenar toda su información en las citadas carpetas y éstos no puedan almacenar información en el escritorio de su estación de trabajo (PC).
- ✓ Los usuarios no deberán de dejar sobre el escritorio físico documentación alguna; por lo que, si debiera hacerlo, deberá de cubrirlo con un folio hasta el final de la jornada laboral.

8.15. USO ADECUADO Y CONSERVACIÓN DE RECURSOS

- ✓ La Subgerencia de Desarrollo y Soporte Informático coordinará con la empresa encargada del mantenimiento preventivo y correctivo de los equipos de cómputo en calidad de alquiler, la realización de estas tareas.
- ✓ Para las computadoras de propiedad de la SBLM, deberá de dar cumplimiento al plan de mantenimiento anual.
- ✓ La adquisición de los bienes (hardware y software) se realizará de conformidad con las directrices y normativas técnicas que establezca la Gerencia de Logística.
- ✓ Todos los equipos tecnológicos deben ser objeto de mantenimiento preventivo, de conformidad con un cronograma preestablecido por el grupo interno de trabajo de la Subgerencia de Desarrollo y Soporte Informático.
- ✓ La empresa encargada del mantenimiento preventivo y correctivo del equipo de cómputo será la responsable del soporte y buen funcionamiento de los equipos de cómputo de la red de la SBLM bajo la supervisión de la Subgerencia de Desarrollo y Soporte Informático, según los términos establecidos en la contratación del servicio y deben asegurar que las condiciones de medio ambiente en que operan éstos se ajustan a las establecidas por la SBLM.
- ✓ La Subgerencia de Seguridad e Infraestructura Informática deberá de contar con documentación actualizada sobre los componentes y organización de las redes de la SBLM, así como de los recursos asociados a éstas, entre otros: enlaces y dispositivos de conexión físicas, protocolos de comunicaciones y direcciones IP, segmentaciones de la LAN extendida y canales de comunicación de las sedes externas.
- ✓ Los requerimientos para la instalación y actualización de las redes de datos deben ser formalizados y controlados adecuadamente, asegurando que su ejecución no interfiera con la operación normal de los servicios.

8.16. SEGURIDAD FÍSICA, ACCESO A CENTRO DE DATOS Y CABLEADO

- ✓ Se encuentra restringido el acceso físico de personas ajenas a las diferentes oficinas de la SBLM en las que se encuentre equipamiento de cómputo en general.
- ✓ Las nuevas edificaciones o remodelaciones donde se ubique equipos de cómputo y de comunicaciones deben considerar dentro de su diseño, los requerimientos de seguridad que dicte la Gerencia de Tecnologías de la Información y Comunicaciones.
- ✓ Las medidas de seguridad física aplican a todos los colaboradores de la SBLM y a terceras personas que por razones calificadas y/o servicios contratados tengan acceso a áreas restringidas.
- ✓ Todos los colaboradores que laboren o visiten áreas de acceso restringido, deberán portar el carnet de identificación suministrado por la SBLM en un lugar claramente visible.
- ✓ Las personas ajenas a la Institución que visiten áreas restringidas deben portar una identificación y una autorización para transitar por dicho lugar.
- ✓ El ingreso y permanencia de personal externo por efectos de tareas de mantenimiento y reparación de equipos deberá contar con la supervisión permanente de un colaborador autorizado del área.

- ✓ Cuando un colaborador extravíe o le haya sido robada su identificación de acceso físico a cualquier área restringida, deberá reportarlo a la Subgerencia de Servicios Generales y al Gerente del área en forma inmediata.

Jr. Carabaya 641, Lima - Perú
(01) 427 6521 / (01) 427 6522

www.beneficenciadelima.org

Beneficencia
de Lima
—1834

Siendo el día miércoles 14 de agosto de 2024 de 2024 los miembros del Directorio, acordaron llevar a cabo su Sesión No presencial N.° 022-2024, desarrollándose el despacho agendado, respecto a la aprobación de la Política de Seguridad Informática de la Sociedad de Beneficencia de Lima Metropolitana, luego de la exposición respectiva, los miembros del Directorio emitieron el siguiente acuerdo:

ACUERDO DE DIRECTORIO N.° 030-2024

VISTO:

El Memorando N.° 111-2024-GTI/SBLM de fecha 08 de mayo de 2024 de la Gerencia de Tecnologías de la Información y Comunicaciones; el Memorando N.° 039-2024-GPD/SBLM de fecha 24 de junio de 2024 de la Gerencia de Planeamiento y Desarrollo, el Memorando N.° 152-2024-GTI/SBLM de fecha 26 de junio de 2024 de la Gerencia de Tecnologías de la Información y Comunicaciones, el Informe N.° 018-2024-SGPI-GPD/SBLM de fecha 01 de julio de 2024 de la Subgerencia de Planeamiento y Proyectos de Inversión; el Memorando N.° 040-2024-GPD/SBLM de fecha 02 de julio de 2024, de la Gerencia de Planeamiento y Desarrollo, el Informe N.° 149-2024-SGAL-GAL/SBLM de fecha 31 de julio de 2024 de la Subgerencia de Asuntos Legales Corporativos; el Informe N.° 051-2024-GAL/SBLM de fecha 31 de julio de 2024 emitido por la Gerencia de Asesoría Legal; y,

CONSIDERANDO:

Que, en el marco del Decreto Legislativo N.° 1411, las Sociedades de Beneficencia son personas jurídicas de derecho público interno, de ámbito local provincial, con autonomía administrativa, económica y financiera y conforme al artículo 4° de la citada norma, las Sociedades de Beneficencia no se constituyen como entidades públicas.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA
SECRETARÍA GENERAL

Que, mediante Memorando N.° 152-2024-GTI/SBLM de fecha 26 de junio de 2024 , la Gerencia de Tecnologías de la Información y Comunicaciones, remitió el proyecto de Política de Seguridad Informática de la Sociedad de Beneficencia de Lima Metropolitana, el mismo que permitirá que los activos de la información que se procesan dentro de la infraestructura tecnológica de la Sociedad de Beneficencia de Lima Metropolitana, se encuentren protegidos con un nivel mínimo de riesgo a la seguridad de la información digital.

Que. mediante Memorando N.° 040-2024-GPD/SBLM de fecha 02 de julio de 2024, la Gerencia de Planeamiento y Desarrollo da conformidad al Informe N.° 018-2024-SGPI-GPD/SBLM de fecha 01 de julio de 2024 emitido por la Subgerencia de Planeamiento y Proyectos de Inversión, el mismo que concluye que la aprobación de la "Política de Seguridad de la Información" contribuye con el Objetivo Estratégico N.° 07- Implementar la transformación digital en la organización y la Acción Estratégica N.° 07.04- Implementar la Seguridad de los Sistemas e Infraestructura Informática.

Que, mediante Informe N.° 051-2024-GAL/SBLM de fecha 31 de julio de 2024, la Gerencia de Asesoría Legal da conformidad al Informe N.° 149-2024-SGAL-GAL/SBLM de fecha 31 de julio de 2024, emitido por la Subgerencia de Asuntos Legales Corporativos, el mismo que considera que el proyecto de "Política de Seguridad Informática" se encuentra alineado a la naturaleza de la Sociedad de Beneficencia de Lima Metropolitana, así como al PEI 2024-2027

Jr. Carabaya 641, Lima - Perú
(01) 427 6521 / (01) 427 6522

www.beneficenciadelima.org

Beneficencia
de Lima
—1834

y a las funciones de responsabilidad designadas en el Manual Estructural Orgánico y Funcional de la Sociedad de Beneficencia de Lima Metropolitana.

Que, la "Política de Seguridad Informática" logrará fijar mecanismo y procedimientos que se deben adoptar por la institución, para salvaguardar sus sistemas y la información que esos contienen, permitiendo contribuir con el objetivo de proteger los activos más sensibles de la institución.

Con el pronunciamiento favorable de la Gerencia de Tecnologías de la Información y comunicaciones, Gerencia de Planeamiento y Desarrollo, de la Gerencia de Asesoría Legal, con la conformidad de la Gerencia General; al amparo de lo dispuesto en el Reglamento del Directorio de la Sociedad de Beneficencia de Lima Metropolitana, RE N.° 001-2022-P-SBLM y de acuerdo al artículo 5° y 7° del Decreto Legislativo N.° 1411, el Directorio como el órgano de mayor nivel de las Sociedades de Beneficencia y en el uso de los poderes y atributos legales que le son inherentes; por unanimidad:

ACORDÓ:

APROBAR la Política de Seguridad Informática de la Sociedad de Beneficencia de Lima Metropolitana.

DISPONER que la Gerencia General, la Gerencia de Tecnologías de la Información y Comunicaciones y demás gerencias competentes, implementen la Política de Seguridad Informática y realicen todas las acciones que fueren pertinentes, con el fin de dar cumplimiento al presente acuerdo.

DISPENSAR del trámite de aprobación de Acta al presente Acuerdo.

SOCIEDAD DE BENEFICENCIA DE LIMA METROPOLITANA
JAIME AUGUSTO TERCERO VARGAS MONTENEGRO
Secretario General