DIRECTIVA				
Código de documento normativo	**Versión N°**	**Total, de Páginas**	**Resolución de Aprobación**	**Fecha de Aprobación**
DIR-001-2024-EMAPE/GTI	02	13	Resolución de Gerencia General N° -2024-EMAPE/GG	Noviembre 2024

DIRECTIVA

SEGURIDAD DE LA INFORMACIÓN DE EMAPE S.A.

RUBRO	NOMBRE	CARGO	FIRMA
FORMULADO POR	JAIME BARNETT PALOMINO	Gerente de Tecnologías de la Información (e)	Firmado digitalmente por BARNETT PALOMINO Jaime FAU 20100063337 soft Motivo: Soy el autor del documento Fecha: 28.11.2024 15:42:12 -05:00
REVISADO POR	JAIME BARNETT PALOMINO	Gerente Central de Administración y Finanzas	Firmado digitalmente por BARNETT PALOMINO Jaime FAU 20100063337 soft Motivo: Soy el autor del documento Fecha: 28.11.2024 16:21:23 -05:00
REVISADO POR	JULIO ALBERTO VÁSQUEZ DÍAZ	Gerente de Planificación Estratégica y Modernización (e)	Firmado digitalmente por VASQUEZ DIAZ Julio Alberto FAU 20100063337 soft Motivo: Soy el autor del documento Fecha: 28.11.2024 17:15:48 -05:00
REVISADO POR	JULIO ALBERTO VÁSQUEZ DÍAZ	Gerente Central de Planificación y Presupuesto	Firmado digitalmente por VASQUEZ DIAZ Julio Alberto FAU 20100063337 soft Motivo: Soy el autor del documento Fecha: 28.11.2024 17:15:59 -05:00
REVISADO POR	FABIAN FELIX SUSANIBAR TELLO	Gerente Central de Asesoría Jurídica	Firmado digitalmente por SUSANIBAR TELLO Fabian Felix FAU 20100063337 soft Motivo: Soy el autor del documento Fecha: 28.11.2024 17:41:31 -05:00
APROBADO POR	CARLOS ENRIQUE PEÑA ORELLANA	Gerencia General	Firmado digitalmente por PEÑA ORELLANA Carlos Enrique FAU 20100063337 soft Motivo: Soy el autor del documento Fecha: 28.11.2024 21:00:30 -05:00

HOJAS DE CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Responsable
01	27-11-2024	Actualización de la denominación social, según Acta de Junta General de Accionistas de fecha 06 de octubre de 2022.	Gerente de Tecnologías de la Información
		Se cambió la estructura de la Directiva de acuerdo al Anexo 4 de la DIR-001-2023/EMAPE/GCPP.	
		Se realizaron modificaciones en los numerales 3.12, 3.13, 5.2.1 y 5.2.2, 5.3, 8.4.3, 8.5.2, 8.5.3, 8.8.1, Anexo 1 y Anexo 2.	

SEGURIDAD DE LA INFORMACIÓN DE EMAPE S.A.

I. OBJETIVO

Normar la administración de la Seguridad de la información, que permita lograr los niveles de protección y control de acceso a los recursos informáticos dentro de la Empresa Municipal de Apoyo de Proyectos Estratégicos - EMAPE S.A.

II. FINALIDAD

Lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información institucional, con el objetivo de asegurar la continuidad operacional de los procesos y servicios que desarrolla la Empresa Municipal de Apoyo a Proyectos Estratégicos – EMAPE S.A.

III. BASE NORMATIVA

3.1 Ley N° 27309, Ley que incorpora los Delitos Informáticos al Código Penal.
3.2 Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, su reglamento y sus modificatorias.
3.3 Ley N° 27815, Ley del Código de Ética de la Función Pública, su reglamento y sus modificatorias.
3.4 Ley N° 28612, Ley que norma el uso y adquisición del software en la Administración Pública, su reglamento y modificatorias.
3.5 Ley N° 29733, Ley de Protección de Datos Personales, su reglamento y sus modificatorias.
3.6 Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano y establecen disposiciones adicionales para el desarrollo del Gobierno Digital y sus modificatorias.
3.7 Decreto Supremo N°050-2018-PCM, que establece la definición de Seguridad Digital.
3.8 Decreto Supremo N° 004-2019- JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.
3.9 Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD que aprueba la Directiva Nº 001-2023-PCM/ SGTD, Directiva que establece el Perfil y Responsabilidades del Oficial de Seguridad y Confianza Digital.
3.10 Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en la Entidades Públicas.
3.11 Resolución Ministerial N° 246-2007-PCM, que aprobó el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información, 2da. Edición” en todas las Entidades integrantes del Sistema Nacional de Informática.
3.12 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.

3.13 Resolución Ministerial N°041-2017-PCM, que aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISP/IEC 12207:2016 – Ingeniería de Software y Sistemas, Proceso de Ciclo de vida de Software, 3ra Edición" en todas las entidades integrales del Sistema Nacional de Informática.

3.14 Resolución de Gerencia General N° 000101-2023-EMAPE/GG, que aprueba la Directiva "Formulación, Aprobación y Modificación de Documentos Normativos; y, Elaboración de Documentos Oficiales en la Empresa Municipal de Apoyo a Proyectos Estratégicos S.A. - EMAPE S.A."

3.15 Resolución de Gerencia General N°000110-2023-EMAPE/GG, que aprueba la modificación del Reglamento de Organización y Funciones de la Empresa Municipal de Apoyo a Proyectos Estratégicos Sociedad Anónima – EMAPE S.A, Resolución de Gerencia General N° 000066-2024-EMAPE/GG y Resolución de Gerencia General N° 000071-2024-EMAPE/GG se emiten sus modificatorias.

IV. ALCANCE

La presente directiva es de aplicación y cumplimiento obligatorio para todo el personal que preste servicios en EMAPE S.A., cualquiera sea su régimen contractual y laboral, que utilicen equipos informáticos.

V. RESPONSABILIDAD

5.1 Es responsabilidad del Gerente de Tecnologías de la Información -GTI:

5.1.1 Asegurar los niveles adecuados de confidencialidad, integridad y disponibilidad de los sistemas de información de los datos y de telecomunicaciones de EMAPE S.A.

5.2 Es responsabilidad de los titulares de los órganos de EMAPE S.A:

5.2.1 Solicitar los accesos de creación, renovación, bloqueo, anulación, y acceso de recursos de red de los usuarios de su Gerencia u órgano mediante formulario digital del Software de Gestión de Servicios – GLPI.

5.2.2 Informar a la GTI sobre los usuarios que dejan de laborar y, en general, que dejen de prestar servicios en EMAPE S.A. para realizar un respaldo o backup de información y los bloqueos a todos los accesos administrativos, mediante el formulario digital del Software de Gestión de Servicios – GLPI.

5.3 Es responsabilidad del usuario reportar a la GTI, cualquier anomalía física y/o lógica de los sistemas o equipos informáticos a su cargo, mediante el Software de Gestión de Servicios - GLPI, para que el personal especializado de la Gerencia de Tecnologías de la Información efectúe las acciones correctivas que permitan solucionar los incidentes reportados.

5.4 El usuario es responsable de las supervisiones del uso adecuado de los recursos de los sistemas y equipos asignados pudiendo coordinar acciones de control (backups) de su información.

5.5 La Gerencia de Logística es responsable de establecer cláusulas de protección y confidencialidad contractuales a los contratos de EMAPE S.A.

VI. DEFINICIONES Y/O SIGLAS

Para efectos de la presente directiva, se entenderá por:

6.1 **Área Usuaria:** Es la dependencia que cuenta con todos los conocimientos técnicos.

6.2 **Centro de Datos:** espacio que sirve para alojar el conjunto de equipos de tecnología

6.3 **Confidencialidad:** Principio fundamental de seguridad que busca garantizar toda la información de las personas, y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o divulgación accidental, sabotaje, y otras acciones que pudieran poner en riesgo dicha información.

6.4 **Cuenta Administrador:** Son los accesos que te permiten realizar todos los cambios que afecten a otros usuarios.

6.5 **Disponibilidad:** Es el principio fundamental de la seguridad que busca garantizar que los usuarios autorizados tengan acceso a la información. Para ello se debe procurar que la información y la capacidad de procesamiento sean resguardados y puedan ser recuperados en forma rápida y completa ante cualquier hecho contingente que interrumpa la operatividad o medios de almacenamiento.

6.6 **Estación de Trabajo:** Área destinada para que un usuario de la red pueda acceder a la misma mediante dispositivos de red (Pc's, Laptop, tablet, teléfono, etc.).

6.7 **Firewall:** Normalmente conocido como barrera cortafuegos. Es un filtro en software o hardware que controla todas las comunicaciones entrantes y salientes de una red a otra red, cuya función principal es denegar o permitir el acceso de dicha comunicación.

6.8 **Información:** La información es un activo que, al igual que otros activos importantes, es esencial para una organización y en consecuencia debe ser protegido adecuadamente. La información puede ser almacenada de muchas formas, incluyendo: forma digital (por ejemplo, en archivos de datos almacenados en medios electrónicos u ópticos), forma material (por ejemplo, en papel), así como información de conocimiento técnico de los servidores.

6.9 **Integridad:** Principio fundamental de seguridad, busca garantizar la precisión, suficiencia y validez de la información, métodos de procesamiento y todas las transacciones de acuerdo con los valores y expectativas de la organización, así como evitar fraudes y/o irregularidades de cualquier índole que haga que la información no corresponda a la realidad.

6.10 **LAN (Local Área Network):** Red de Área Local, tipo de arreglo para comunicación de datos a alta velocidad (típicamente en el rango de los Mbit/s) en donde todos los segmentos del medio de transmisión (cable de par trenzados, o fibras ópticas) están circunscritos a una región geográficamente reducida.

6.11 **Malware:** Se define como software malicioso que cubre un amplio rango de software hostil como son los virus, gusanos, caballos de troya, etc., capaces de causar daños o alteraciones del sistema operativo, archivos, u otros componentes de computadoras y redes informáticas.

6.12 **Perfil:** Conjunto de facultades que se le atribuyen a los usuarios del sistema que permiten determinar la atribución de sus funciones, en razón de sus posibilidades de accesos al sistema y de gestión privilegios.

6.13 **Protocolo:** Conjunto de reglas conocidas y respetadas que en los extremos de un enlace de telecomunicaciones que regulan las transmisiones en todos los sentidos posibles.

6.14 **Recursos Informático:** Equipamiento de Hardware tales como: computadoras, servidores, impresoras, escáneres, etc., y herramientas de Software ya sean estos programas de terceros, herramientas de internet o software desarrollados dentro de la organización.

6.15 **Respaldo:** Es una copia de seguridad es un proceso mediante el cual se duplica la información existente.

6.16 **Seguridad de la Información:** Conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de la información.

6.17 **Soporte Técnico:** Servicio que se brinda a todos usuarios de EMAPE S.A. cuenta con herramientas en hardware y software que le permite colaborar en la resolución de cualquier tipo de problemas.

6.18 **SPAM:** Se define como Correo Electrónico “tipo basura” o también conocido como “correo no solicitado”. Estos mensajes son normalmente enviados a través de listas de correo invisibles o grupos de noticias que bombardean con propaganda de todo tipo de productos o servicios. Muchos de estos mensajes vienen infectados de virus, gusanos y caballos de Troya

6.19 **Usuario:** Son los Trabajadores y, en general, cualquiera que preste servicios en EMAPE S.A., ya sean nombrados o contratados bajo cualquier régimen, que utilizan los equipos informáticos de la Empresa.

6.20 **Virus:** Programa malicioso, escrito intencionalmente para auto instalarse en la computadora de un usuario sin conocimiento o permiso de éste. Se comporta como un programa parásito porque infecta y ataca a los archivos contenidos en el computador. Para propagarse, se replica a sí mismo ilimitadas veces, llegando a producir serios daños que pueden afectar a los sistemas y archivos en general, pudiendo estos últimos daños borrar, corromper o destruir dichos archivos.

6.21 **VPN (Virtual Private Network):** Red Privada Virtual construida dentro de una red pública mediante protocolos que reservan su uso a un grupo restringido de usuarios

6.22 **GLPI:** Software de gestión de servicios donde se ha desarrollado la gestión de atención de la mesa de ayuda.

VII. DISPOSICIONES GENERALES

7.1 La Gerencia de Tecnologías de la Información, evaluará y aprobará las solicitudes de acceso a los servicios informáticos:

- Conectividad a la Red de Datos y Comunicaciones.
- Correo electrónico (Interno o vía Web).
- Sistemas informáticos.
- Internet.
- Acceso a Conexiones remotas Seguras.

- Telefonía (anexos)

7.2 Toda información proporcionada a los usuarios es de carácter exclusivo para el desarrollo de sus actividades, es confidencial y no puede ser empleada en beneficio propio o de terceros, salvo la información clasificada como pública y de acuerdo al procedimiento correspondiente.

7.3 La Gerencia de Logística debe establecer en los contratos a suscribir por EMAPE S.A. según corresponda clausulas relacionado con la seguridad de la información.

7.4 Las funciones propias del usuario determinarán los recursos y servicios informáticos a los que podrá disponer; estas funciones serán determinadas por la Gerencia o el órgano al cual pertenece.

7.5 Toda información creada y modificada por los usuarios de EMAPE S.A., como parte de sus funciones y actividades, es de total propiedad de la Institución.

7.6 A fin de establecer niveles de acceso a la información en las carpetas compartidas, esta se clasifica como:

- Nivel de Acceso Total, cuando el usuario tiene el acceso de crear, editar y eliminar.
- Nivel Escritura, cuando el usuario solo puede editar más no borrar.
- Nivel Lectura, cuando el usuario solo puede leer, más no editar ni eliminar.

7.7 Los Órganos de Alta Dirección, Órgano de Control, Órgano de Asesoramiento, Órgano de Apoyo y Órganos de Línea de EMAPE S.A. son los responsables directos del buen uso de la información en sus respectivas unidades orgánicas.

VIII. DISPOSICIONES ESPECÍFICAS

8.1 Equipo Informático

8.1.1 La Gerencia de Tecnologías de la Información, es responsable de registrar los equipos informáticos (CPU, Teclado, etc.) de acuerdo a los códigos de inventario asignado por la oficina de control patrimonial.

8.1.2 La Gerencia de Tecnologías de la Información, es responsable de instalar, configurar y mantener los equipos informáticos asimismo la asignación de las direcciones IP (Protocolo de Internet).

8.1.3 Los usuarios no están autorizados a instalar ningún software.

8.1.4 Los usuarios no están autorizados a realizar cambios en las configuraciones de red de los equipos a su cargo.

8.1.5 Cada usuario de red contará con una identificación de usuario (LOGIN) y una clave de acceso (PASSWORD), credenciales necesarias para acceder a los equipos informáticos.

8.1.6 Los equipos informáticos serán configurados como objetos de dominio de la Institución.

8.1.7 El inicio de sesión en los equipos de dominio deberá ser sólo a través de las credenciales proporcionadas por la Gerencia de Tecnologías de la Información.

8.1.8 Ningún usuario podrá tener privilegios de administrador en su equipo ni acceder con alguna cuenta de administrador.

8.1.9 Por seguridad, la cuenta administradora local de los equipos informáticos siempre permanecerá deshabilitada.

8.1.10 Los usuarios son responsables de bloquear sus respectivos equipos de cómputo (PC), cuando se ausenten momentáneamente de su puesto de trabajo; para ello deben pulsar las teclas “Control”, “Alt” y “Supr”, y luego seleccionar la opción “Bloquear”. Esto impide tanto el acceso no autorizado al sistema, como a las aplicaciones. El usuario que no deje bloqueado su computador al ausentarse será responsable por el uso no autorizado del equipo e información.

8.2 Correo Electrónico

8.2.1 Cada trabajador de EMAPE S.A. cuenta con una identificación de usuario (LOGIN) y una clave de acceso (PASSWORD), los cuales posibilitan su acceso a los servicios de la red. Estos parámetros son personales, confidenciales e intransferibles.

8.2.2 Cada usuario es responsable de su cuenta, y toda la información que se emite a través de esta.

8.2.3 El Correo Electrónico es de uso exclusivo para las actividades propias relacionadas con las funciones de cada trabajador o con los alcances de los servicios para los que es contratado.

8.2.4 Al pie de cada mensaje los usuarios deberán enviar una identificación que permita conocer al autor del mensaje, con la finalidad de que permita al receptor de datos identificarlo formalmente.

8.2.5 Los usuarios de correo electrónico de EMAPE S.A., no deben ser utilizados para lo siguiente:

- Enviar cadena de mensajes.
- Enviar mensajes relacionados a seguridad, exceptuando al personal encargado de la administración de la seguridad de la información.
- Enviar propaganda de candidatos políticos.
- Actividades ilegales, no éticas o impropias.
- Otra información que cuenta con prohibiciones legalmente expresa.

8.2.6 Toda la información recibida, transmitida y almacenada en los servidores de correo electrónico institucionales es considerada propiedad de EMAPE S.A.

8.3 Uso de Software

8.3.1 La Gerencia de Tecnologías de la Información tiene como responsabilidad establecer mecanismos de restricciones de acceso por perfiles para:

- La Instalación de Software
- Acceso al panel de control y otras opciones de configuraciones de las computadoras.

8.3.2 La instalación de software en una PC, debe ser solicitado por el Gerente responsable de la Gerencia a la que pertenece el usuario final, el software debe ser instalado únicamente por el personal de la Gerencia de Tecnologías de la Información.

8.3.3 La Gerencia de Tecnologías de la Información, es el encargado de tener una bitácora de registro de cada software, su actualización y estado.

8.4 De las contraseñas de seguridad

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

8.4.2 La contraseña es asignada por el usuario al momento de activar su cuenta, por lo tanto, nadie más que el usuario conoce dicha contraseña.

8.4.3 Para garantizar la confidencialidad de la información en la red de EMAPE S.A. el usuario deberá asignar una contraseña que debe tener lo siguiente:

- Una combinación de letras mayúsculas, letras minúsculas y números. No deben ser palabras comunes o simples variaciones como nombre del trabajador, mascotas, etc. Por ejemplo, una contraseña fuerte puede ser: Jwp05T4-8.
- Cambiar la contraseña con mayor frecuencia y cuando el usuario sospeche que la seguridad de su contraseña puede estar comprometida o vulnerable e informar a la Gerencia de Tecnologías de la Información a través del Software de Gestión de Servicio - GLPI, para la evaluación y tomar acciones correspondientes.

8.4.4 A partir de la activación de la cuenta y establecimiento de la contraseña, el usuario asume la responsabilidad sobre la inviolabilidad de esta. El propietario de la cuenta de usuario es el único responsable del uso que se le dé a ésta, siendo la cuenta de usuario y su contraseña, de carácter personal e intransferible, queda totalmente prohibido compartirlas para ser usados por otras personas.

8.5 De los Centros de Datos

Para su acceso físico y/o lógico se ha establecido lo siguiente:

8.5.1 El entorno que debe contar el Centros de Datos de EMAPE S.A. deben ser áreas seguras, protegidas por perímetros de seguridad definidos, controles de entrada y acceso apropiados para prevenir la exposición a riesgos de sabotaje, robo de información y de los recursos de tratamiento de información y evitar pérdidas, daños o comprometer la actividad y continuidad de estos.

8.5.2 Los equipos y servidores de la infraestructura informática de EMAPE S.A. están ubicados en el local principal de la Institución de Vía Evitamiento Km 1.7, Lima 15023 - EMAPE S.A.

Protección contra ataques informáticos, virus y malware

La Gerencia de Tecnologías de la Información, es responsable de la instalación del antivirus, que reduzca la probabilidad de una infección directa

en las computadoras; esta solución debe contar con repositorios remotos para la replicación de las actualizaciones.

8.5.3 Queda terminantemente prohibido a los usuarios finales la descarga de archivos y/o programas de tipos: ejecutables (*.exe, *.msi, etc.), de música y videos en todos sus formatos, pues pueden contener virus, spyware, gusanos y malware en general; los cuales podrían perjudicar la seguridad de la información de la Empresa. En caso se requiera algún programa de tipo gratuito, deberá ser solicitado a la Gerencia de Tecnologías de la Información mediante el Software de Gestión de Servicio - GLPI, especificando el motivo de la necesidad y en que computadora serán instalados, previa evaluación de riesgo.

8.5.4 Los usuarios finales deberán tener mucho cuidado en que los dispositivos que traigan (USB, CD, DVD, memoria externa etc.) no hayan sido utilizados en otras computadoras infectadas.

8.5.5 Actualmente EMAPE S.A cuenta con una solución “antispam” que impide la propagación de mensajes maliciosas que tengan adjuntos archivos potencialmente peligrosos, contenidos para adultos, phishing, etc.

8.5.6 El antivirus instalado en EMAPE S.A. está compuesta por módulos que protegen computadoras, así como el servicio de correo electrónico, todo está gestionado de manera centralizada mediante una consola de antivirus, que cuenta con repositorios remotos para replicación de las actualizaciones.

8.5.7 Si un computador detecta una infección o malware en progreso, el personal de la Gerencia de Tecnologías de la Información está facultado a tomar el control y mitigar los efectos del malware.

8.6 Del Respaldo de Seguridad

8.6.1 La Gerencia de Tecnologías de la Información, dispone de un sistema de respaldo de información para minimizar los daños y proteger la información procesada, al nivel de base de datos, aplicaciones, configuraciones de los sistemas operativos y de comunicaciones.

8.6.2 Los usuarios que tienen asignada una computadora, son responsables de grabar su información trabajada de la información producida.

8.6.3 Se realizarán copias de seguridad de la información, de acuerdo a la disponibilidad de los servidores y se efectuarán de tres formas.

- Respaldo Completo: Copia completa de información
- Respaldo Incremental: Copia de todos los cambios o adicionales que se realizan a determinada información
- Respaldo Diferencial: Copia de cambios o adicionales que se realizan a determinada información respecto al respaldo completo, después de cierto periodo de tiempo.

Para atender las solicitudes de copias de respaldo de seguridad de la información de tomaran en cuenta los siguientes criterios:

- Solo los documentos institucionales y

- De acuerdo a la disponibilidad de los servidores.

8.7 Sistema de Redes

Con relación a los sistemas de la red local y de conectividad a internet:

8.7.1 Debe tenerse en consideración las técnicas de seguridad que se evalúen como convenientes: Cortafuegos, Proxy, autentificación; que permitan controlar la seguridad de los usuarios de la red local y del sistema de conectividad a internet.

8.7.2 Se debe tener actualizado la estructura de la red de datos y comunicaciones, identificando locales, equipos utilizados e información relevante para su supervisión.

8.7.3 Se efectuarán bloqueos dadas las acciones de control en los equipos, sobre el bloqueo de programas como Facebook, Twitter, YouTube y otros que la entidad y/o consideren necesario limitar, se considerará como falta de parte del usuario, el vulnerar dichas configuraciones a fin de recuperar dichos accesos.

8.8 Gestión de Servidor Web y Servidor de Correo Electrónico

8.8.1 La Gerencia de Tecnologías de la Información, deshabilitará las cuentas de los sistemas de información de uso en EMAPE S.A. y dominio a usuarios que dejaron de prestar servicios a EMAPE S.A. para tal fin la Gerencia u órgano usuario deberá comunicar a través del Software de Gestión de Servicios – GLPI, dentro de las 48 horas del término del vínculo contractual producida.

8.8.2 La Gerencia de Tecnologías de la información, será responsable de la validación de servicio de datos y otros procesos, para garantizar los servicios de manera permanente.

8.9 Acceso Remoto

8.9.1 Los accesos remotos serán habilitados a solicitud de las Gerencias usuarias.

8.9.2 El usuario del acceso remoto deberá observar de manera estricta de disposiciones descritas en la presenta directiva.

8.9.3 La Gerencia u órgano usuario supervisará el buen uso del acceso remoto habilitado.

8.9.4 Adicionalmente a disposiciones de la presenta directiva el usuario debe proteger la información a la que tiene acceso de amenazas como, el acceso no autorizado, alteración indebida o software malicioso cumpliendo con lo siguiente:

- Conectarse desde ambientes físicos y seguros
- Cuando se retira de su ubicación bloquear el equipo con el teclado presionando Windows + L.
- Conectarse desde accesos a internet confiable, no público o gratuito y salvaguardar en todo momento su usuario y contraseñas.

IX. DISPOSICIONES COMPLEMENTARIAS

9.1 La Gerencia de Tecnologías de la Información, podrá emitir disposiciones específicas y efectuar precisiones respecto a la presente directiva, de acuerdo a las normas vigentes.

9.2 La situación no contemplada en la presente será resuelta por la Gerencia de Tecnologías de la Información.

9.3 Adicionalmente se deberá tener en cuenta la adecuación a cualquier norma legal que se establezca con posterioridad a la fecha de aprobación de la presente directiva.

9.4 La Gerencia de Tecnologías de la información, podrá precisar los procedimientos no contemplados en la presente directiva.

X. ANEXOS

- Anexo N° 01 – Imagen del formulario digital de solicitud de cuenta de usuario que es realizado a través del Software de Gestión de Servicios - GLPI

IMAGEN DEL FORMULARIO DIGITAL DE SOLICITUD DE CUENTA DE USUARIO EN EL SOFTWARE DE GESTIÓN DE SERVICIOS - GLPI