EPYSA PERU SAC

1. CONCEPTOS GENERALES.

La información utilizada por EPYSA PERU SAC, sea información de clientes o información propia de la Empresa, debe ser considerada como uno de sus activos más importantes. Esta información puede existir en muchas formas, puede estar impresa o escrita en papel, almacenada electrónicamente, ser transmitida manualmente o por medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiera la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada, ya que la información lleva riesgos operativos no únicamente asociados a los sistemas y tecnologías de la información.

La seguridad de la información que permite mantener la disponibilidad, integridad y confidencialidad de la información, es esencial para conservar la ventaja competitiva, cumplir con las normas legales y proteger la imagen de la Empresa. Nuestra información y los sistemas que la soportan pueden ser el objetivo de diversas amenazas como fraudes, sabotaje, espionaje industrial, vandalismo, ataques de hackers y de virus informáticos; amenazas en continua expansión que hacen que nuestra información y sistemas informáticos estén expuestos a riesgos cada vez mayores.

La seguridad de la información que permite mantener la disponibilidad, integridad y confidencialidad de la información, es esencial para conservar la ventaja competitiva, cumplir con las normas legales y proteger la imagen de la Empresa. Nuestra información y los sistemas que la soportan pueden ser el objetivo de diversas amenazas como fraudes, sabotaje, espionaje industrial, vandalismo, ataques de hackers y de virus informáticos; amenazas en continua expansión que hacen que nuestra información y sistemas informáticos estén expuestos a riesgos cada vez mayores.

La seguridad de la información busca fundamentalmente, alcanzar los siguientes objetivos:

CONFIDENCIALIDAD

La información sólo debe ser conocida por el personal que la requiera para el desarrollo de sus funciones.

Este objetivo busca garantizar que toda la información de clientes, directores y empleados, y sus medios de procesamiento y/o conservación, estén protegidos del uso no autorizado o revelaciones accidentales, sabotaje, espionaje industrial, violación de la privacidad y otras acciones que pudieran poner en riesgo dicha información.

INTEGRIDAD

Este objetivo busca garantizar que toda la información de clientes, directores y empleados, y sus medios de procesamiento y todas las transacciones se encuentren libres de errores, fraude y/o irregularidades de cualquier índole que haga que la información no corresponda a la realidad.

DISPONIBILIDAD

La información debe estar disponible para el personal, clientes, directores y entidades reguladoras en forma oportuna y acorde a sus niveles de autorización.

Este objetivo busca garantizar que los usuarios autorizados tengan acceso a la información de los recursos relacionados con la misma, de acuerdo a sus necesidades. 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 dañe las instalaciones, medios de almacenamiento y/o equipamiento de procesamiento.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarcan políticas, normativas, procedimientos, estructuras organizacionales y funciones del software.

2. OBJETIVOS DE LA POLÍTICA GENERAL DE SEGURIDAD DE INFORMACIÓN.

Este documento busca establecer el marco global de seguridad de la información que permita lograr los niveles de seguridad que EPYSA PERU SAC requiere en base a las necesidades del negocio.

La Política General de Seguridad de Información y los documentos asociados (normas y procedimientos) tienen los siguientes objetivos:

- Cumplir con los niveles de autorización y responsabilidad sobre la información (utilización, divulgación, administración y custodia), establecidos para el normal desarrollo de las actividades del negocio. Las autorizaciones parten desde la solicitud de la Gerencia General a cada vez mayores accesos a su personal y donde comparte la responsabilidad con cada persona autorizada.
- Minimizar la posibilidad de ocurrencia de hechos contingentes que pudieran interrumpir la operación del negocio y reducir el impacto de los daños a las instalaciones, medios de almacenamiento, equipos de procesamiento y de comunicación.
- Proteger la información, sus medios de procesamiento, conservación y transmisión, del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, violación de la privacidad y otras acciones que pudieran perjudicarla o ponerla en riesgo.
- Establecer, difundir y controlar las normas relacionadas a la protección de la información y sistemas de la Empresa.
- Establecer normas de seguridad sobre los servicios que se realizan con la colaboración de terceros acordes con las políticas de seguridad de la Empresa.
- Cumplir las normas legales y reglamentarias, estipuladas por Ley y los organismos reguladores correspondientes, referidas a seguridad de la información y medios que la contienen.
- Sensibilizar y capacitar a los empleados acerca de su responsabilidad para mantener la seguridad de la información y su adecuado uso, estableciendo una cultura organizacional que incorpore el tema de seguridad de la información como un aspecto relevante en los procesos de negocio de la Empresa.

## 3. ALCANCE.

Este documento y los documentos asociados, establecen la Política General de Seguridad de Información para los usuarios de la Empresa que deberá ser de conocimiento y cumplimiento obligatorio del personal, permanente o temporal, así como del personal de las compañías contratadas por la Empresa en tanto realicen tareas para ésta.

Este documento cubre los siguientes temas:

- Política de Seguridad.
- Organización para la administración de Seguridad de Información.
- Clasificación de activos de información.
- Seguridad física y lógica de los equipos.
- Administración de las operaciones y comunicaciones.
- Controles de acceso.
- Desarrollo y mantenimiento de sistemas.
- Administración de la Continuidad de los Negocios.
- Cumplimiento.

## 4. ORGANIZACIÓN PARA LA ADMINISTRACIÓN DE LA SEGURIDAD DE INFORMACIÓN.

La Empresa cuenta con una estructura que soporta los aspectos de seguridad de información al interior de la organización, la cual considera principalmente los siguientes roles y responsabilidades:

### 4.1. Administrador de Servidores y Redes.

Es la persona designada por la Empresa que tendrá como principales responsabilidades:

- Crear, revisar y coordinar con la Gerencia General, la promulgación de las normativas, controles, procedimientos y responsabilidades generales, asociados a la seguridad de la información.
- Administrar y controlar el plan de implementación de las normativas y controles establecidos y definidas en este documento y otros documentos complementarios.
- Monitorear permanentemente el cumplimiento de las políticas de seguridad de la información.

- Velar por la implementación de los distintos mecanismos de registro de eventos y demás parámetros de seguridad de información a nivel de sistemas operativos y aplicaciones.
- Analizar e informar formalmente a la Gerencia General de cualquier evento que atente contra la seguridad de la información.
- Mantener contacto con terceros, especialmente con compañías de servicio que apoyen a la Empresa en la administración de un evento de seguridad de información.

4.2. Responsable de la Información. (Administrador de Servidores y Redes).

Es la persona designada por la Empresa que tendrá como sus principales responsabilidades:

- Clasificar la información previamente asignada.
- Definir los niveles de autorización y tipos de acceso que podrán tener los usuarios de la organización sobre la información.
- Velar por la calidad de la información.

Dicha responsabilidad no puede ser delegada a terceros, sólo se podrá delegar la custodia de la información en un colaborador perteneciente a un área en particular dentro o fuera de la Empresa, que apoyará en las tareas operativas de administración y control de seguridad correspondientes a la información.

4.3. Usuarios de la Información.

Conjunto de personas internas y/o externas que con la debida autorización del responsable de la información, puede consultar, ingresar, modificar o borrar la información almacenada en los sistemas informáticos u otros medios de almacenamiento.

Los usuarios sólo deben tener acceso a la información a la que están autorizados a consultar y procesar. Las autorizaciones que se otorguen limitarán su capacidad en los entornos informáticos de forma que no puedan realizar actividades diferentes a las autorizadas.

Las principales responsabilidades de los usuarios de información son las siguientes:

- Utilizar la información sólo para el propósito para el que recibió autorización de uso.
- Cumplir los controles establecidos en la normativa interna y externa.
- Tomar las medidas adecuadas para evitar que la información se divulgue o use sin autorización.

4.4. Custodios de Información (Área de Sistemas).

Se denomina custodio de información al personal o área que proporciona servicios de almacenamiento y procesamiento de información a la Empresa. Cabe señalar que los custodios no necesariamente requieren de la información para el desarrollo de su trabajo, éstos la procesan, gestionan su almacenamiento y la hacen accesible a los demás usuarios.

Las principales responsabilidades de los custodios de información son:

- Garantizar el establecimiento y aplicación de los controles establecidos por el responsable de la información.
- Asegurar protección física a la gestión y almacenamiento de la información.
- Garantizar la disponibilidad de la información, participando además en el Plan de Continuidad.
- Garantizar que la información entregada al usuario sea actualizada e íntegra.

4.5. Terceras partes.

- Aquellas compañías contratadas, que deban efectuar tareas críticas para la organización deberán pasar por un proceso de selección riguroso en el que se le indique claramente las responsabilidades que están asociadas a la confidencialidad, integridad y disponibilidad de la información dentro de la organización.
- Los accesos del personal de las compañías contratadas deben estar debidamente controlados y bajo políticas, normas, procedimientos y estándares de la Empresa.

- Asimismo, el intercambio de información y/o software entre la Empresa y aquellas contratadas requiere la existencia de un acuerdo de confidencialidad, seguridad y licenciamiento de software. Dicho acuerdo deberá estar debidamente escrito y firmado. El mismo debe explicar los términos del intercambio, así como la manera en que el software y los datos serán manejados y protegidos. Esta política no cubre el envío de información designada como pública.
- El acceso del personal externo (terceras partes) debe estar debidamente controlado por la Empresa. Las personas que no sean empleados o contratistas de la Empresa no deben contar con un identificador (id) en la red o en los sistemas a menos que se cuente con la autorización adecuada.
- Todo usuario de tercera parte deberá asegurar sus propios sistemas de acuerdo a los estándares de seguridad de la Empresa.
- La Empresa se reserva el derecho de auditar las medidas de seguridad de esos sistemas.
- La Empresa se reserva el derecho de revocar las autorizaciones de acceso a la información de aquellas terceras partes, que no cumplan con las disposiciones antes mencionadas.
- El intercambio de información y/o software entre la Empresa y cualquier entidad externa requiere de la existencia de un acuerdo de confidencialidad y cumplimiento del marco regulatorio de seguridad escrito y firmado. Tal acuerdo debe explicar los términos del intercambio, así como la manera en que el software y los datos serán manejados y protegidos. Esta política no cubre el envío de información designada como pública.

## 5. MARCO NORMATIVO.

### 5.1. Estructura de la Política de Seguridad de la Información.

La documentación de la política de seguridad de la información de la Empresa contempla los siguientes documentos:

- Política General de Seguridad de la Información.
- Normas y Procedimientos.
- Estándares Tecnológicos.

### 5.2. Elaboración y Aprobación.

Las normativas, procedimientos y estándares de la política de seguridad de la información a ser desarrollados al interior de la Empresa, serán elaborados por el Administrador de Servidores y Redes. Estos documentos serán aprobados en base al Workflow.

El Jefe inmediato superior efectuará la revisión y una primera aprobación de las normativas elaboradas y posteriormente la Gerencia General previa evaluación, las aprobará.

### 5.3. Distribución y Publicación.

La Gerencia General y el Administrador de Servidores y Redes publicarán los documentos aprobados.

### 5.4. Vigencia.

El presente marco normativo, entra en vigencia a partir de su promulgación por la Gerencia General. Una vez distribuida y publicada la política se dará por conocida y aceptada.

### 5.5. Capacitación.

Todos los empleados de EPYSA PERU SAC y cuando sea relevante, los usuarios externos, deberán recibir una capacitación adecuada a las funciones que tengan asignadas al interior de la Empresa, la que debe incluir responsabilidades asociadas a la seguridad de información, uso de recursos, responsabilidades legales y controles del negocio; así como entrenamiento en el uso correcto de aplicaciones para el procesamiento de la información. Esta capacitación debe ser actualizada regularmente.

El responsable de Recursos Humanos, debe incorporar en el Plan de Capacitación de la Empresa, el tema de seguridad de información. Éste

en coordinación con el área de Sistemas definirá el alcance e implementación.

Esta capacitación debe ser clasificada según el rol que cumplirá el empleado al interior de la Empresa y debe realizarse en forma clara y con un lenguaje sencillo. Posteriormente esta capacitación debe estar reforzada por comunicados ocasionales sobre el tema.

Se debe mantener registro de los procesos de capacitación a los que ha asistido el empleado.

5.6. Actualización.

La Política General de Seguridad de Información y los documentos complementarios deben ser revisados y actualizados periódicamente.

Se deberá asegurar que la revisión se efectúe acorde a normativas del ente regulador, cambios en el perfil de riesgo original, incidentes de seguridad de información significativos, nuevas vulnerabilidades o cambios en la infraestructura organizacional o técnica.

Las Jefaturas y usuarios de cada área deben proponer y desarrollar nuevas normas y procedimientos.

Cualquier modificación efectuada al marco normativo – PGSI, deberá efectuarse manteniendo el formato establecido por la Empresa, controlando las versiones y contando con la aprobación de los niveles correspondientes.

## 6. POLÍTICA DE SEGURIDAD DE INFORMACIÓN.

### 6.1. Aspectos Generales.

- Todo el personal de la Empresa, tiene el derecho y el deber de conocer sus responsabilidades respecto a la seguridad de la información.
- El personal que efectuara tareas críticas para EPYSA PERU SAC, debe pasar por un proceso de reclutamiento riguroso en el que se le indique claramente las responsabilidades que están asociadas a su función dentro de la Empresa.
- Un requisito fundamental para obtener niveles apropiados de seguridad de información en la Empresa es la colaboración de todo el personal. Para conseguir su participación es imprescindible establecer políticas de sensibilización y concientización que permitan al personal conocer y asumir las políticas de seguridad de información.
- El incumplimiento de las políticas de seguridad de información conducirá a acciones disciplinarias que serán definidas por el área de Recursos Humanos de EPYSA PERU SAC, de acuerdo a la gravedad de la falta.
- Cuando una persona haga uso de su periodo vacacional, él o los usuarios de acceso a los distintos sistemas que utiliza, deberán ser temporalmente deshabilitados para evitar que personal no autorizado intente utilizar dichas cuentas para efectuar alguna acción no autorizada.
- Cuando una persona cesa en la Empresa se deberá tener en cuenta que:
    - El área de Recursos Humanos, deberá notificar al Administrador de Servidores y Redes para que éste cancele todas las cuentas y accesos a los sistemas de información que tenía asignado, esto debe ser efectuado en el momento de haberse producido el desvinculamiento de dicha persona.
    - El área de Recursos Humanos recibirá del personal cesado todos los elementos que la Empresa le suministró para su labor.
- Cuando se trate de un recurso provisto por un proveedor externo, el jefe del área en donde éste laboraba, deberá enviar una comunicación al Administrador de Servidores y Redes indicando que dicha persona ha terminado sus labores en la Empresa y por ende deben revocarse todos los accesos asignados.
- El conocimiento de las área de sistemas, operaciones o cualquier área de la empresa, deben estar en el dominio de dos personas, de forma que se puedan cubrir situaciones inesperadas sin interrumpir el servicio.

  El velar por esta política es responsabilidad de la Gerencia o Jefe inmediato del área que efectúa procesos críticos para la Empresa.

- El personal y contratistas de la Empresa están en la obligación de reportar al Administrador de Servidores y Redes los diferentes incidentes de seguridad de información, tales como fallos en seguridad, amenazas, debilidades de los sistemas, de acuerdo a los procedimientos establecidos.
- Todo el personal interno y/o temporal deben cumplir con los requerimientos de control y seguridad de información especificados en estas políticas y deberán firmar un documento de conocimiento y aceptación de la Política General de Sistemas de Información de la Empresa, el que se detalla más adelante.
- Todo el personal de EPYSA PERU SAC, deberá ser capacitado en el tema de la seguridad de información, con el objeto de lograr un nivel de sensibilización y concientización acorde al tipo de función y responsabilidad que ejerce al interior de la Empresa.

6.2. Seguridad Física y Lógica de los Equipos.

6.2.1. Áreas Críticas (Sala de Servidores).

- Definimos como áreas críticas, a los lugares protegidos bajo controles de entrada. Estas áreas deben de estar físicamente protegidas contra accesos no autorizados, daños e interferencias.
- Los lugares donde se albergan los activos donde se procesa y almacena la información crítica de la Empresa es considerada un área crítica que debe contar con los controles antes mencionados.
- La infraestructura eléctrica y el cableado en general deberán estar convenientemente ordenados a fin de prevenir cortocircuitos y fallos en los equipos. Así mismo, en la Sala de Servidores, los circuitos y redes informáticas deberán estar identificados y rotulados.
- El acceso a las áreas críticas sólo estará permitido a personal autorizado y a los contratistas que realizan mantenimiento a las instalaciones de éstas, los que deberán estar permanentemente supervisados por personal de la Empresa.

6.2.2. Seguridad de los Equipos Informáticos.

- Todos los equipos informáticos de la empresa deberán estar tanto física como lógicamente protegidos.
- Se deben de establecer contraseñas de acceso a las PC o portátiles y protectores de pantalla por periodos de inactividad. En el caso de los portátiles, se deberá implementar los mecanismos de seguridad que correspondan al nivel de criticidad de la información, que se maneja en éstos.

6.3. Administración de las operaciones y comunicaciones.

El personal de EPYSA PERU SAC debe seguir las siguientes políticas para una adecuada administración de sus procesos:

6.3.1. Control de Cambios.

- Toda nueva aplicación o cambio en la plataforma existente, sea cual sea éste, debe ser informado al Administrador de Servidores y Redes con el objeto de verificar que se cuente con una evaluación de los riesgos involucrados en el pase a producción. No se puede pasar a producción sin asegurarse previamente de que no se afectarán ni interrumpirán los procesos habituales.
- Todos los cambios en los sistemas de información deben ser realizados por el Administrador de Servidores y Redes, para lo que debe existir un procedimiento formal, el cual contemple la evaluación del riesgo asociado a dicho cambio y asegure que se efectúen solamente los cambios autorizados por los usuarios involucrados.

6.3.2. Controles preventivos: detección de virus, spam y otros ataques.

- Todas las estaciones de trabajo de EPYSA PERU SAC y demás, que se conecten a las redes internas, deben cumplir con el uso del software antivirus aprobado por la Empresa.

- En caso de ocurrir una infección por virus u otro tipo de ataque sobre una estación de trabajo, el usuario deberá manejarlo como un incidente de seguridad de información, reportándolo al Área de sistemas para que se proceda a solucionar el incidente.
- Los usuarios no deben usar ningún software que no haya sido revisado por el Área de Sistemas, para evitar la infección por virus o ataques de cualquier tipo. Sólo se podrá manejar como excepción el software que haya sido probado y aprobado por el responsable de Redes.
- El archivo de registro de firmas del antivirus o cualquier componente de las herramientas de seguridad instaladas en las estaciones de trabajo, deben ser permanentemente actualizados, bajo responsabilidad del área de Sistemas.
- Los responsables de los controles preventivos del área de Sistemas, deberán emitir un informe mensual de los eventos de virus u otros ataques ocurridos en la plataforma de la Empresa, este informe debe ser entregado a la Gerencia General.

6.3.3. Seguridad sobre las redes.

- Toda conexión externa a la red de la empresa deberá ser autorizada por la Gerencia General y estar acorde a la norma de conexiones externas, así mismo toda la información que se transmita deberá contar con un nivel de seguridad adecuado de acuerdo con su clasificación.
- Las comunicaciones se pueden realizar por líneas propias como por redes públicas. Si bien ambos procedimientos pueden ser utilizados, el nivel de seguridad de las redes públicas es inferior, por lo tanto en ese caso se deberá utilizar procedimientos de seguridad adicionales.
- Con el fin de garantizar un funcionamiento y mantenimiento adecuados, el responsable del mantenimiento de las Redes, debe documentar y mantener actualizado el esquema de la Red de la empresa. Dicha documentación deberá estar a disposición del personal autorizado, cada vez que éste la requiera.

6.3.4. Copias de Respaldo.

- La disponibilidad de los sistemas operativos, aplicaciones en producción y la información de los usuarios (datos) son la parte medular del plan de continuidad de negocio, por lo que es necesario asegurar que se contará con la disponibilidad de dicha información mediante un adecuado procedimiento de respaldo en base a copias de seguridad periódicas, locales y externas, de Software Base, Datos (bases de datos, archivos críticos en disco y cinta) e Inventario de las copias de respaldo realizadas.
- Las copias de respaldo realizadas deberán almacenarse adicionalmente en una ubicación diferente a los sistemas respaldados, que cuente con fácil acceso y niveles de seguridad adecuados, evitando su pérdida en caso de siniestro de gran magnitud y asegurando el acceso adecuado en caso de contingencia.

6.3.5. Seguridad en el correo electrónico.

- El correo electrónico se pone a disposición del personal de EPYSA PERU SAC para el desarrollo exclusivo de sus funciones laborales, el servicio de correo puede ser proporcionado tanto a nivel interno como externo.
- Se debe tener en cuenta que en la mayor parte de casos el almacenamiento de los mensajes se realiza en las escaleras de trabajo de los usuarios, por lo cual, estarían disponibles a cualquier persona que accede a dicha estación. Por lo tanto, se deberán tomar las medidas adecuadas para proteger el acceso a sus estaciones de trabajo.
- Todo correo electrónico que contenga información confidencial deberá tener en el Asunto “subject” la palabra CONFIDENCIAL, a modo de rotulación.

- Sólo personal debidamente autorizado tendrá la potestad de enviar mensajes de correo electrónico en representación de EPYSA PERU SAC a ámbitos fuera del entorno de la Empresa.

6.3.6. Seguridad en Internet.

- El acceso a internet se provee como una herramienta para el desarrollo exclusivo de la actividad laboral del personal de EPYSA PERU SAC. El acceso deberá ser aprobado por la Gerencia o Jefatura respectiva.
- El acceso a internet, por parte de los usuarios internos, requerirá que éstos estén debidamente identificados y conectados en los sistemas de red.
- Todas las conexiones a internet deberán estar controladas mediante la instalación de mecanismos de control de acceso a la red de la empresa y servidores que soportan los servicios de internet que entrega la misma. Los programas que se usen para estos servicios deberán de ser aprobados por la Gerencia General y se permanentemente actualizados, evaluados e instalados los parches de seguridad que se generen por parte de los fabricantes, en caso que la evaluación defina que se deben instalar.

6.4. Control de Accesos.

- La autorización de acceso a la información, por parte de los usuarios debe ser realizada de acuerdo con sus atribuciones, funciones y/o tareas a desarrollar. Estas deben ser asignadas por la gerencia correspondiente. Será responsabilidad del Jefe directo definir el perfil de acceso de sus subordinados.
- Será responsabilidad del jefe directo definir el personal de reemplazo temporal para las funciones y tareas desarrolladas en su área, para periodos de vacaciones y licencias médicas. El acceso realizado por el personal de respaldo (backup) deberá ser efectuado utilizando su cuenta personal, no puede utilizar la cuenta de la persona que reemplaza.
- El acceso a los recursos de información de EPYSA PERU SAC es a través de usuarios y contraseñas. El Administrador de Servidores y Redes es el responsable de la creación, administración y eliminación de los usuarios. Estas tareas deben estar acordes al procedimiento del Mantenimiento de usuarios de la Red y Correo Electrónico.
- El acceso a las aplicaciones deberá estar adecuadamente restringido sólo para usuarios con autorización, así mismo las aplicaciones deben contar con una adecuada estructura de perfiles de usuario que restrinja los accesos de acuerdo a las funciones y responsabilidades de los empleados de la Empresa.

6.4.1. Monitoreo y uso de los sistemas de acceso.

- En la medida que el software del sistema lo permita, los sistemas de comunicaciones y servidores que contengan información sensible, valiosa o crítica de la Empresa deberán contar con un registro de eventos de seguridad de información relevante, para detectar lo siguiente:
  - Intentos de adivinar contraseñas.
  - Intentos de usar privilegios no autorizados.
  - Cambios a privilegios de usuarios.
  - Modificaciones a software de sistemas.
- Los eventos de seguridad antes mencionados deberán ser almacenados por lo menos 30 días, y deben ser permitidos a sólo personal autorizado. Estos eventos serán de mucha utilidad para la corrección de errores, recuperación de violaciones de seguridad e iniciativas relacionadas.

6.4.2. Acceso por parte del Área de Soporte Técnico.

- El personal del área de Soporte Técnico está autorizado, previo consentimiento del usuario para revisar archivos de los usuarios con el propósito de resolver problemas inesperados tales como los generados por virus o caídas del sistema. En tal

caso están obligados a notificar a los usuarios que se ha tomado tal acción. Si se efectuaron copias de los archivos éstas deben destruirse.

- El Gerente o Jefe inmediato o a quién él designe en su reemplazo, podrán hacer uso de herramientas de hardware y/o software que pudieran evaluar o comprometer la seguridad de los sistemas de información, previa autorización de la Gerencia General y para propósitos de evaluar la seguridad delos sistemas. Esta autorización deberá ser otorgada por un periodo de tiempo limitado.

6.4.3. Control de Cumplimiento de la PGSI.

Dado que EPYSA PERU SAC pone a disposición de los empleados internos o externos, los recursos de la información con el objeto de que éstos desarrollen su trabajo y funciones asignadas y que estas facilidades son sólo entregadas para que sean utilizadas para el propósito del negocio, se considera que los empleados no manejan información personal, por lo que los siguientes procesos de monitoreo y control son responsabilidad y derecho de la Empresa:

- La Gerencia General o quién ésta delegue se reserve el derecho de examinar todos los datos guardados o transmitidos en sus sistemas, correo electrónico, directorios de archivos personal, disco duro, y cualquier otra información mantenida o transmitida en los sistemas de la Empresa. Esta revisión se realizará para asegurar la conformidad con las políticas de seguridad, para el apoyo a la ejecución de investigaciones internas y para ayudar al control de la administración de los sistemas de la información.
- La Empresa se reserva el derecho de supervisar, accesar, recuperar, leer, y/o descubrir comunicaciones del personal cuando:
  - Exista una verdadera necesidad comercial que no pueda ser satisfecha a través de otros medios.
  - El personal involucrado no está disponible y el tiempo sea crítico para una actividad comercial.
  - Exista una causa razonable para sospechar de una actividad delictiva o violación a las políticas de seguridad.
  - Sea requerida por la ley o regulación, para una supervisión.

6.5. Desarrollo y Mantenimiento de Sistemas.

6.5.1. Requerimientos de Seguridad de Información.

- Los sistemas desarrollados por EPYSA PERU SAC o contratados a terceros por la Empresa, deberán contar con un módulo de seguridad el cual garantice una adecuada administración de usuarios/contraseñas e implemente una estructura de perfiles que permita controlar el acceso al sistema y a la información.
- Adicionalmente los sistemas deberán de contar con un registro de eventos de seguridad para una adecuada revisión posterior a algún incidente.
- Los requerimientos de seguridad deben estar incorporados desde un inicio al proceso de desarrollo, sean éstos desarrollos internos o externos.

6.5.2. Seguridad en el desarrollo y procedimientos de soporte.

- El desarrollo de sistemas se debe realizar en ambientes estrictamente controlados y diferentes a los de producción, el Responsable de Sistemas es responsable de la seguridad y ambiente para el adecuado desarrollo.
- Los programas fuente de las aplicaciones de la Empresa deberán estar adecuadamente resguardados y sólo deben ser accesibles por el personal autorizado.

6.5.3. Administración de la continuidad de los negocios.

- EPYSA PERU SAC debe contar con un Plan de Continuidad del Negocio, que busque contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos del negocio de las consecuencias de faltas significativas y desastres.
- Se debe contar con planes de contingencia que permitan garantizar que los procesos de negocio sean restaurados dentro de los plazos requeridos por la Empresa.
- El Plan de Continuidad de Negocio y el Plan de Contingencia, deben ser evaluados, validados y actualizados en forma periódica.

6.6. Cumplimiento.

6.6.1. Cumplimiento con los requerimientos legales.

- EPYSA PERU SAC operará siempre dentro del marco legal al que se encuentra sometido, manteniendo siempre como premisa, asegurar el cumplimiento de los objetivos de la Empresa, actuar de acuerdo con las políticas generales de la Empresa y mantener siempre un comportamiento profesional y de compromiso con la calidad.
- La información almacenada en los archivos informáticos de la Empresa es básica para el funcionamiento del negocio y estará adaptada a lo que las leyes en vigor dictamen. Nunca podrá ser usada sin autorización previa, ni con fines distintos a los requeridos por el trabajo encomendado en cada momento.
- Tanto el software adquirido por EPYSA PERU SAC, como los programas desarrollados en forma interna están sujetos a la normativa sobre propiedad intelectual.
- Sólo se podrá utilizar software autorizado por el Área de Sistemas.

6.6.2. Cláusulas de Confidencialidad.

- Toda vez que se confíe información crítica a un tercero, debe procurarse contar con un acuerdo por escrito de confidencialidad, no divulgación y uso apropiado de la información entregada por EPYSA PERU SAC. Este acuerdo debe incluir instrucciones precisas para el manejo de los datos y la eliminación o borrado de los mismos cumplido el periodo circunstancial que llevo a confiar en el tercero.
- En el caso que se requiera que la Empresa firme un acuerdo de confidencialidad con terceros, éste sólo podrá ser firmado por el Gerente General o quién él designe en su defecto.

6.6.3. Legalidad de Software.

- El responsable de Sistemas centralizará la administración y supervisión de las licencias de software de las estaciones de trabajo de los usuarios de la Empresa.
- El responsable de Sistemas debe efectuar inventarios periódicos del Software instalado en los equipos del personal de la Empresa. En aquellos casos en que se detecte anomalías o software no autorizado, se informará al Jefe inmediato involucrado y al Administrador de Servidores y Redes, quienes coordinarán con Recursos Humanos la aplicación de medidas correctivas según Reglamento Interno de la Empresa.
- La instalación de software en los ambientes de procesamiento y/o estación de trabajo, sólo puede ser llevada a cabo por personal autorizado o por los mecanismos automáticos destinados a dicho fin.

6.6.4. Derechos de propiedad intelectual.

- Se debe asegurar que el software de EPYSA PERU SAC (adquirido o desarrollado internamente) y su utilización cumpla con la normativa legal vigente, correspondiente a decreto legislativo 822, Ley de Derechos de Autor.
- Los productos (software u otros productos) desarrollados o modificados internamente por personal de EPYSA PERU SAC, son de propiedad exclusiva de la Empresa.
- El software desarrollado internamente por personal de la Empresa, deberá inscribirse a nombre de EPYSA PERU SAC,

en el registro de propiedad intelectual respectivo, con el objeto de acogerse a los resguardos que estipula la Ley de Propiedad Intelectual.

- No se podrá prestar ni copiar software adquirido o desarrollado por la Empresa a no ser que exista una autorización de la Gerencia General.
- Es recomendable que todo el Software y la documentación que posea la Empresa incluya avisos de los derechos de autor y propiedad.
- EPYSA PERU SAC tiene la propiedad legal sobre el contenido de todos los archivos almacenados en los equipos de cómputo y sistemas en red, así como de todos los mensajes que viajan a través de estos sistemas. La Empresa se reserva el derecho de permitir el acceso a esta información a terceras personas.
- Los usuarios finales no deberán copiar el software proporcionado por la Empresa en ningún medio de almacenamiento magnético o divulgar software sin autorización escrita correspondiente.

6.6.5. Faltas a la Política.

- La seguridad de la información en todos sus ámbitos, debe ser considerada como un ítem dentro de la evaluación de desempeño del personal.
- El incumplimiento de las obligaciones y prohibiciones mencionadas en este documento y otros documentos complementarios, facultan a EPYSA PERU SAC a aplicar medidas disciplinarias definidas por el área de Recursos Humanos y de acuerdo a la gravedad de la falta.

6.6.6. Responsabilidades.

- La satisfactoria implementación de la PGSI de la Empresa sólo podrá lograrse con la cooperación y ayuda de todos los empleados, por lo tanto, es necesario que todo el personal este sensibilizado y comprometido con los requerimientos de seguridad de información identificados, dado que éstos son responsables del cumplimiento de estas políticas.
- Será responsabilidad del trabajador que detecte un incumplimiento de las obligaciones o prohibiciones indicadas en este documento, dar a conocer en forma inmediata al Área de Sistemas, área que centralizará todos los eventos de seguridad de la información y los derivará al Administrador de Servidores y Redes, si corresponde. Dicho Administrador gestionará la investigación del hecho y reportará a la Gerencia, el resultado de dicha investigación. En caso de comprobarse una inconducta, el Área de Sistemas, dará aviso a Recursos Humanos para que tome las acciones pertinentes.
- Es responsabilidad de la Gerencia General de la Empresa, asegurar que el personal reciba una adecuada capacitación relacionada a seguridad de información y se comprometa a cumplir con dichos procedimientos. Las Jefaturas son responsables de asegurar que sus empleados o el personal externo que trabaja en su área, conozcan y cumplan dichas políticas.
- EPYSA PERU SAC, podrá supervisar violaciones a las políticas mediante controles en base a los cuales se podrán tomar medidas disciplinarias.

7. ANEXOS Y DEFINICIONES.

Definiciones.

**Activos de Información**, es todo recurso de información, software, físico o servicio que contenga y/o manipule información de EPYSA PERU SAC.

**El marco normativo o Política de Seguridad de la Información**, es un conjunto de documentos formales, que se aplican de manera funcional y genérica a cualquier tarea, industria, actividad o disciplina y que ayudan a la Gerencia General en la dirección y guía de los empleados en la terminación efectiva de sus deberes.

Bajo esta definición el marco normativo de EPYSA PERU SAC, es un conjunto de políticas, normas y procedimientos, estándares usados para comunicar sus estrategias al resto de la organización.

**Las Políticas**, son las reglas a las que se deben ajustar las tareas y actividades relacionadas con la protección de la información; estas son independientes del ambiente de procesamiento.

**Las Normativas**, son reglas concretas que definen cursos de acción precisos para las distintas tareas que se desarrollan dentro de la Empresa.

**Los Procedimientos**, son la forma particular de lograr algo o actuar. Son los pasos que debe realizar el personal para dar cumplimiento a una norma. Se entiende por procedimientos al detalla de tareas pendientes a ejecutar y controlar algunas de las funciones administrativas u operativas de la Empresa, señalando los responsables de la ejecución y control.

**Los Estándares**, son documentos específicos de un departamento, producto o proceso. Son las instrucciones o valores particulares que deben aplicarse a cada ambiente de procesamiento / documentación en cada proceso. Se entiende como estándares al conjunto de parámetros lógicos o físicos determinados, los que se consideran como valores específicos del tema en cuestión.

**Recursos de Hardware**, equipamiento tecnológico constituido por equipos portátiles, equipos de escritorio, discos, equipos de comunicación, servidores, cortafuegos, etc.

Software, conjunto de programas o aplicación informáticos desarrollados o adquiridos por la Empresa.

**Usuarios**, son las personas tanto internas como externas a la Empresa, que hacen uso de los recursos informáticos y de la información de ésta con el objeto de poder cumplir con sus correspondientes funciones.