MANUAL DE ORGANIZACIÓN

SECCION:

GERENCIA DE INFORMATICA

SIGET

SUPERINTENDENCIA GENERAL DE
ELECTRICIDAD Y TELECOMUNICACIONES

CONTENIDO

Sección 04 **Departamento en Seguridad Informática.**

01 Jefe de Departamento en Seguridad Informática
02 Técnico en Seguridad Informática.

CAPITULO VI Listado de Distribución, Revisiones y Ediciones.

Sección 00 Sección Única

SECCION 01 SECCION ÚNICA

La Gerencia se encuentra ubicada en el nivel de staff, dependiendo directamente del Superintendente.

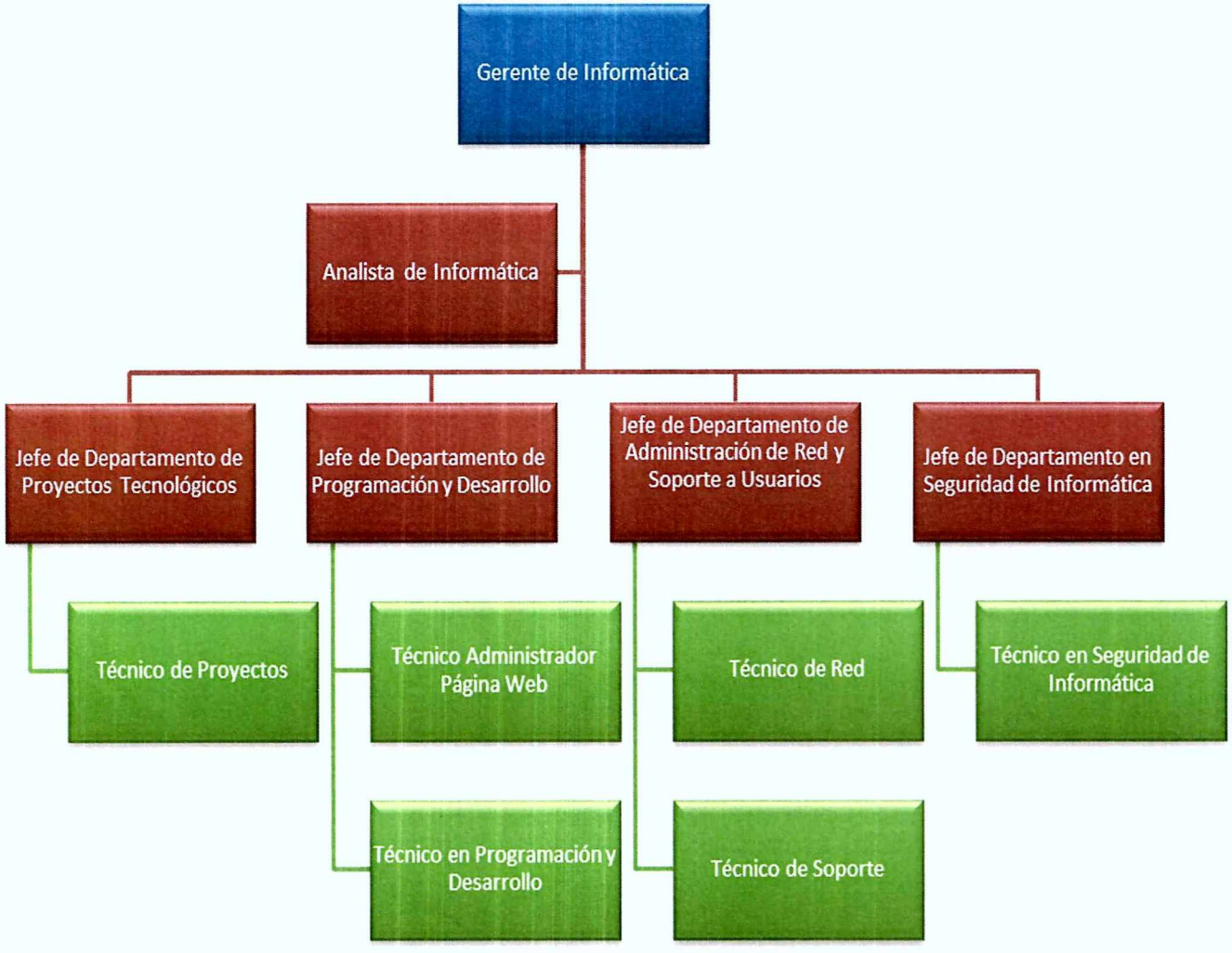
La relación de la Gerencia con el resto de la organización es de apoyo sobre las actividades de cada área de trabajo.

La autoridad que la Gerencia de Informática ejerce se limita al personal que la integra.

A continuación se presenta el organigrama por puestos de trabajo.

SECCION 02 ESTRUCTURA ORGANIZATIVA

GERENCIA DE INFORMÁTICA



SECCIÓN 03 ESTRATEGIAS Y POLITICAS DE LA GERENCIA DE INFORMATICA (GI)

ESTRATEGIAS

Procurar mantener la actualización tecnológica de acuerdo a los recursos disponibles y necesidades de la SIGET, optimizando el uso de los mismos.

POLITICAS DE TECNOLOGIAS, INFORMACIÓN Y COMUNICACIÓN.

POLÍTICAS GENERALES PARA LA SEGURIDAD INFORMATICA.

A.- Organización de la Seguridad Informática.-

1.- El objetivo principal de la Seguridad Informática será proteger desde el ámbito tecnológico la información electrónica institucional, los recursos informáticos y los servicios tecnológicos necesarios para que la SIGET pueda cumplir con las funciones y obligaciones que le correspondan de acuerdo a la normatividad aplicable.

2.- La Seguridad Informática en la SIGET implica una responsabilidad de todos los empleados de la institución, pero de manera especial a los administradores, usuarios de Sistemas y Servicios Informáticos Institucionales.

3.- La Gerencia de Informática es el área responsable de coordinar acciones para determinar la plataforma tecnológica; y establecer lineamientos, estándares, criterios, medidas y otras disposiciones técnicas, en materia de Seguridad Informática.

4.- El Titular de la Gerencia de Informática será además el coordinador de la Seguridad Informática y designará a un Responsable de la Seguridad Informática de la SIGET quienes serán los responsables de las labores relacionadas con la Seguridad Informática de la Institución.

5.- El Coordinador de Seguridad Informática de la SIGET, tendrá las siguientes responsabilidades:

a) Proponer e integrar estrategias y elementos para conformar el Programa Institucional de Seguridad Informática alineados a un enfoque de seguridad de la Información, en coordinación con el Responsable de la Seguridad Informática y los Enlaces Informáticos

b) Coordinar los procesos y proyectos en materia de Seguridad Informática con los Enlaces Informáticos y con el Responsable de Seguridad Informática de la SIGET;

c) Mantener la coordinación en materia de Seguridad Informática con el área encargada de la Gestión documental y con el área administrativa encargada de acceso a los edificios de la Institución;

d) Establecer acuerdos en materia de Seguridad Informática con áreas internas e instituciones externas a la SIGET;

e) Proponer recomendaciones y acciones de aplicación general en materia de Seguridad Informática;

f) Proponer criterios en materia de Seguridad Informática para la clasificación, registro y protección de los recursos informáticos de la SIGET;

g) Publicar en la Intranet Institucional los documentos normativos en materia de Seguridad Informática como representante del Comité de Seguridad Informática de la SIGET previa autorización de Superintendente;

h) Designar los responsables de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática.

6.- El Responsable de la Seguridad Informática de la SIGET, será el encargado de:

a) Coordinar con los responsables de servicio las acciones en materia de Seguridad Informática que deberán llevarse a cabo en la SIGET;

b) Proponer políticas y especificaciones técnicas de bienes y servicios, procedimientos, acciones y medidas específicas en materia de Seguridad Informática la Gerencia de Informática; que sean aplicables a cualquiera de los elementos tecnológicos que integren la plataforma de Seguridad Informática de la Institución;

c) Mantener la administración del sistema de autentificación de usuarios que permite el acceso a los recursos y servicios informáticos y de comunicaciones de la SIGET;

d) Coordinar la definición, la administración y las acciones técnicas en materia de Seguridad Informática con personal de la Gerencia, los responsables de servicios, los administradores de servicios y con otras áreas que realicen funciones informáticas para la Institución;

e) Del sistema de gestión de incidentes de seguridad de la información, analizar aquellos que involucren los servicios informáticos a fin de establecer controles para detectar, corregir y prevenir incidentes posteriores.

f) Proponer medidas específicas en materia de Seguridad Informática que deberán atender los usuarios de los bienes, de los recursos y servicios informáticos y de la información electrónica;

g) Proponer la plataforma tecnológica para el soporte del ambiente de Seguridad Informática de la SIGET;

h) Mantener actualizado el inventario de Activos Informáticos relacionados con la Plataforma de Seguridad Informática de la SIGET como complemento del inventario de activos de Información;

i) Realizar revisiones selectivas a los controles de los activos informáticos para asegurar que se mantenga sobre ellos la aplicación de las recomendaciones y lineamientos en materia de Seguridad Informática;

j) Establecer en coordinación con el departamento de Red y Soporte a usuarios y los responsables de servicio las ubicaciones y condiciones con que deberá realizarse el respaldo de la información electrónica;

k) Publicar en la Intranet Institucional los documentos técnicos en materia de Seguridad Informática emitidos por el Comité de la Seguridad Informática de la SIGET previa autorización de su Jefe inmediato y Superintendente;

l) Promover el cumplimiento de la normatividad informática en la SIGET;

m) Definir controles de detección y prevención para la protección contra software malicioso;

n) Implementar controles para la protección contra software malicioso en la infraestructura de cómputo y telecomunicaciones;

o) Definir las cuentas de acceso para la administración de los equipos de cómputo para proteger la configuración de los mismos, las cuales hará del conocimiento a los Enlaces Informáticos;

p) Revisar los registros de eventos de los diferentes equipos que formen parte del ambiente de seguridad de la SIGET a fin de colaborar con el responsable del servicio en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad;

q) Coordinar, administrar y registrar todos los nombres de equipos y dominios que son accesibles en la Intranet y en Internet de la SIGET;

r) Controlar y registrar todos los certificados de seguridad de los sitios de la SIGET;

s) Promover la cultura de la Seguridad Informática entre los administradores y usuarios de la información electrónica y de los recursos, bienes y servicios informáticos institucionales (promover una cultura de prevención); y

t) Las demás que determine el Jefe de Seguridad Informática.

7.- Para facilitar las tareas de planeación y coordinación de la Seguridad Informática se establece un Comité de Seguridad Informática integrado por el Coordinador de Seguridad Informática, el Responsable de Seguridad Informática, Jefes de departamentos de la Gerencia.

8.- El Comité de Seguridad Informática será coordinado por el Gerente de la Gerencia de Informática, y tendrá como Secretario al responsable de la Seguridad; y los demás miembros serán considerados como vocales.

9.- Cada miembro del Comité de Seguridad Informática tendrá derecho a voz y voto y en caso de empate el voto del coordinador del grupo será considerado como voto de calidad.

10.- El Comité de Seguridad Informática tendrá las siguientes funciones:

a) Realizar ejercicios de análisis de riesgos de acuerdo a la metodología establecida en el Sistema de Seguridad de la Información(Unidad de Gestión Documental), ya sea con recursos propios o a través de contratación externa;

b) Elaborar y dar seguimiento de los Planes de Continuidad que van a ejecutar el Grupo de Operación de Seguridad Informática;

c) Aprobar las medidas generales de Seguridad Informática;

d) Aprobar el Programa Institucional de Seguridad Informática

e) Aprobar estrategias en materia de Seguridad Informática;

f) Determinar el listado de Activos Informáticos relacionados con la plataforma de Seguridad Informática;

g) Aprobar la plataforma tecnológica para sustentar el ambiente de Seguridad Informática;

h) Designar las Áreas de Acceso Informático Restringido y a los responsables de controlar su acceso;

i) Evaluar el desempeño del ambiente de Seguridad Informática;

j) Realizar propuestas para mejorar el ambiente de Seguridad Informática; y

k) Las demás que determine el Titular de la Institución.

11.- La Gerencia de Informática (GI) deberá implementar y ejecutar las tareas, acciones y medidas en materia de Seguridad Informática acordadas por el Comité de Seguridad de la Información Institucional

12.- La Gerencia de Informática tendrá las siguientes funciones en materia de seguridad informática:

a) Cumplir el Programa Institucional de Seguridad Informática;

b) Mantener un sistema de monitoreo y seguimiento del desempeño del ambiente de Seguridad Informática.

c) Realizar estudios y propuestas para mejorar el desempeño del ambiente de Seguridad Informática;

d) Apoyar en el diseño y modificaciones de la plataforma tecnológica que soporta al ambiente de Seguridad Informática;

e) Acordar acciones técnicas tendientes a mejorar el desempeño del ambiente de Seguridad Informática;

f) Establecer grupos de trabajo específico para analizar en conjunto con los Responsables de la Información Electrónica Institucional, los riesgos de los accesos de terceros a la información de la Institución y proponer medidas con el propósito de minimizar sus posibles efectos negativos;

g) Proponer a los responsables de cada uno de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática de la SIGET;

h) Establecer medidas para el control de acceso físico y lógico a las áreas designadas como de acceso restringido;

i) Establecer el programa de ejercicios de análisis de riesgos de los activos informáticos que deberán realizar los responsables de servicios y los enlaces

j) informáticos, para garantizar su continuidad y para contribuir al Sistema de Seguridad de la Información para este fin;

k) Elaborar e implementar Planes de Continuidad necesarios para atender eventualidades que puedan afectar la continuidad de las actividades de la Institución;

l) Coordinar las tareas definidas en los Planes de Continuidad;

m) Realizar ensayos, mantenimiento y reevaluación de los Planes de Continuidad;

n) Dar a conocer al personal involucrado todo cambio realizado al plan de contingencia;

o) Implementar los procedimientos, requerimientos y medidas que deberán atender los responsables, administradores y usuarios de servicios informáticos para utilizar los recursos tecnológicos que sean responsabilidad de la SIGET; y

p) Las demás que determine el Comité de Seguridad de la Información Institucional.

1. **El personal de la Gerencia de Informática tendrán las siguientes responsabilidades con respecto a la Seguridad Informática en la Institución:**

a) Atender las disposiciones en materia de Seguridad Informática que se emitan en la SIGET y promover el cumplimiento al interior de su Unidad Administrativa;

b) En coordinación con el Responsable de Seguridad Informática y los responsables de servicios, realizar ejercicios de análisis de riesgos que contribuyan a la continuidad operativa de los Servicios Informáticos y de Seguridad de la Información.

c) Verificar que se cumplan las condiciones establecidas por la Institución para proteger los Activos Informáticos relacionados con la Plataforma de Seguridad Informática de la SIGET que se encuentren asignados a su Unidad Administrativa;

d) Proporcionar información sobre los registros de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática de la SIGET

e) Atender en coordinación con el responsable de Seguridad Informática cualquier hecho que ponga en riesgo el Ambiente de Seguridad Informática en su Unidad Administrativa;

f) Verificar las condiciones del Ambiente de Seguridad Informática y proponer a la GI medidas para mejorarlo;

g) Verificar que todo equipo o medios de almacenamiento sujeto a reutilización que contenga información sensible sean borrados de forma permanente antes de su reasignación; y

h) Aquellas adicionales que determine la Gerencia de informática.

B. - Administración de los Activos Informáticos.-

1.- El Coordinador de Seguridad Informática emitirá el listado de Activos Informáticos relacionados con la Plataforma de Seguridad Informática.

2.- El Responsable de la Seguridad Informática deberá diseñar, implementar y mantener un inventario actualizado de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática de la SIGET conforme al listado de Activos Informáticos que apruebe el Comité de Seguridad Informática.

3.- La Gerencia de informática propondrá un responsable para cada uno de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática que se encuentren relacionados en el inventario mencionado en el numeral anterior.

4.- El Comité de Seguridad Informática designará a cada uno de los responsables de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática de la SIGET.

5.- Los responsables de los Activos Informáticos relacionados con la Plataforma de Seguridad Informática del SIGET, deberán atender las siguientes funciones relacionadas con el activo del que sean responsables:

a) Mantener la información actualizada del activo en el registro correspondiente al activo informático del que sean responsables;

b) Establecer esquemas de protección del activo acordes a las recomendaciones, políticas y lineamientos que sean emitidos por el Comité de Seguridad Informática;

c) Atender a las medidas y disposiciones acordadas por el Comité de Seguridad Informática.

C.- Responsabilidades en Materia de Seguridad Informática para el Uso de Bienes, Servicios, Recursos Informáticos y de Información Electrónica.-

1.- Todo Usuario de Recursos Informáticos tendrá las siguientes responsabilidades:

a) Atender las medidas de Seguridad Informática emitidas por la Institución que se encuentren publicadas en la Intranet Institucional;

b) Mantener bajo reserva las claves de usuario y los correspondientes códigos de acceso que le hayan sido asignadas por la Institución;

c) Bloquear el acceso a su equipo de cómputo cuando deba dejarlo desatendido por algún tiempo;

d) Almacenar de manera segura (bajo llave) las computadoras portátiles y Soporte Móvil de Almacenamiento Informático removible, en gabinetes u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo, o bien asegurar con cable de bloqueo o algún otro medio que evite la sustracción no autorizada de las computadoras portátiles que se encuentren bajo su resguardo;

e) Verificar que las condiciones del lugar donde realiza sus labores sean las adecuadas para evitar que los recursos informáticos y la información bajo su resguardo pudieran ser sustraídos por terceros no autorizados y en caso de no contar con las condiciones adecuadas informar a su Enlace Informático;

f) Abstenerse de instalar software sin previa justificación, notificación y autorización de su Enlace Informático;

g) Solicitar a través del Responsable de la Seguridad o soporte informático el apoyo para desinstalar el software del que sospeche que tiene una anomalía;

h) Realizar respaldo de la Información Electrónica bajo su responsabilidad para la continuidad de sus funciones; o solicitar a soporte informático realice el mismo.

i) Reportar al Responsable de la Seguridad a través de soporte Informático cualquier situación que considere que puede poner en riesgo el Ambiente de Seguridad Informática de la Institución.

2.- Todo Usuario de Activos Informáticos deberá cumplir las siguientes reglas de uso de contraseñas:

a) Mantener las contraseñas en secreto;

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas;

c) Seleccionar contraseñas de calidad, de acuerdo a las indicaciones informadas por el Responsable del Servicio de que se trate, y cuidando que:

i. Sean fáciles de recordar.

ii. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

iii. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

iv. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

d) Cambiar las contraseñas provisionales en el primer inicio de sesión; Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro;

e) Notificar directamente al responsable seguridad informática en su ámbito de competencia cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

f) No anotar sus contraseñas en los equipo o en otros lugares visibles para los demás usuarios, se recomienda memorizar su contraseña y evitar escribirla en cualquier lugar,

g) Las contraseñas son personales e intransferibles por lo que no podrá compartir sus contraseñas.

h) No iniciar sesión con su usuario en otros equipos que no sea el asignado a menos que la situación lo amerite.

i) Las claves de acceso deben tener las siguientes características:

- Combinaciones de letras y números,
- Son compuestas por mínimo 6 caracteres.
- Restablecimiento de contraseñas al menos cada dos meses.
- No se habilitan los accesos automáticos a los portales bancarios (usuarios y contraseña).

3.- El uso de recursos del personal o de terceros (Proveedores, Clientes, etc.) para el procesamiento de información en el lugar de trabajo debe ser controlado según el procedimiento de Seguridad Informática establecido y autorizado.

4.- Todo Usuario que haga uso de equipo de cómputo o dispositivos móviles de la Institución debe atender los Procedimientos y Políticas de Seguridad de Equipos de Cómputo Portátil y Comunicaciones Móviles.

5.- Toda persona que desempeñe actividades para apoyar las funciones de la SIGET y que para sus tareas requiera hacer uso de activos informáticos de la Institución, tendrán las siguientes responsabilidades:

a) Asistir a los cursos de capacitación en materia de Seguridad Informática que gestione la institución y que el Comité de Seguridad Informática determine como obligatorios;

b) Establecer las medidas necesarias para proteger la información electrónica que se encuentre bajo su resguardo, conforme a la normatividad vigente;

c) Mantener activos y bajo la configuración asignada los sistemas de Seguridad Informática proporcionados por la Institución sobre los bienes, servicios e información a los que tenga acceso;

d) Realizar un respaldo de la Información electrónica bajo su responsabilidad al cambiar de: equipo asignado para el desempeño de sus actividades, de funciones, de área de adscripción o al finalizar su relación con la Institución, y entregarlo de manera formal a su Jefe Inmediato que haya estado encargado de supervisar sus funciones;

e) Notificar a soporte de Informática cualquier cambio: de equipo, de funciones, o de área de adscripción para que se apliquen las medidas de Seguridad Informática correspondientes;

6.- La Gerencia de informática a través del Departamento de Red y Soporte a Usuarios deberá asegurar que todos los equipos que dejen de ser utilizados temporal o permanentemente no contengan información institucional, sean formateados y contengan solamente la imagen original del Sistema Operativo con que fueron adquiridos y que sea desinstalado todo el software que requiera del pago de licenciamiento por parte de la SIGET.

7.- Toda persona que requiera retirar de las instalaciones del SIGET algún equipo de cómputo o comunicaciones o software deberá contar con la autorización formal (por escrito y validada) de su área administrativa correspondiente o según el procedimiento que exista para ello.

8.- Toda aplicación desarrollada por la Institución o por un tercero para la SIGET debe tener un responsable único designado formalmente, de acuerdo a lo establecido en las políticas y normatividad institucional sobre desarrollo de sistemas informáticos y deberá tramitarse su inscripción en el Centro Nacional de Registro.

9.- Todo Usuario de Recursos Informáticos y Usuario Externo deben de reportar los incidentes de seguridad a su jefe inmediato superior, al encargado del área donde presta su servicio o la Gerencia de Informática, tan pronto hayan tomado conocimiento de su ocurrencia.

10.- Los Usuarios de Sistemas y Servicios Informáticos, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de Seguridad Informática, son responsables de registrar y comunicar inmediatamente las mismas al Departamento de Red y Soporte a Usuarios.

11.- El Usuario de Recursos Informáticos no debe realizar pruebas para detectar y/o utilizar una supuesta debilidad o falla de Seguridad Informática.

12.- Todo Usuario de Recursos Informáticos que detecte una anomalía de software en producción deberá:

a. Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
b. Alertar al Departamento de Red y Soporte a Usuarios.

D.-. Ambiente de Seguridad Informática de la SIGET.-

1.- Todo incidente o violación de la Seguridad Informática debe ser reportado al Área de Seguridad Informática o al Departamento de Red y Soporte a Usuarios para su investigación y resolución del incidente.

2.- Los responsables de servicios informáticos deberán apoyar la implementación de las medidas de control y acceso a las Áreas de Acceso Informático Restringido.

3.- El responsable de Seguridad Informática con el apoyo de los responsables del control de acceso a las Áreas de Acceso Informático Restringido deberá mantener un registro foliado correlativamente de dichas áreas en el que se identificarán la ubicación, las condiciones físicas, los activos informáticos a proteger y las medidas de protección física y lógicas aplicables.

4.- Los responsables del control de acceso a las Áreas de Acceso Informático Restringido deberán establecer las medidas de seguridad que deberán atender quienes accedan a ellas.

5.- El ingreso a las Áreas de Acceso Informático Restringido será autorizado en conjunto por el responsable del control de acceso a dichas áreas y el responsable de Seguridad Informática correspondiente.

6.- El ingreso o salida a las Áreas de Acceso Informático Restringido de equipos electrónicos, de cómputo, de almacenamiento, de comunicaciones, accesorios y otros dispositivos deberá ser autorizado por el responsable del control de acceso al área informática restringida, el responsable de Seguridad Informática y el Responsable de Activo Fijo y siempre deberán encontrarse relacionadas a un responsable de ellos que será la persona encargada de solicitar el movimiento.

7.- Cualquier persona que sea externa a la Institución no podrá acceder, ni permanecer en ninguna de las Áreas de Acceso Informático Restringido si no se encuentra acompañado por un empleado de la SIGET y que además cuente con la autorización para su ingreso.

8.- Queda prohibido comer, beber y fumar dentro de cualquiera de las Áreas de Acceso Informático Restringido.

9.- Para cada Área Informática restringida el responsable de control de acceso deberá mantener un registro, que deberá hacer del conocimiento del responsable de la Seguridad Informática, de las personas autorizadas para acceder de manera temporal o permanente.

10.- Los responsables del control de acceso a las Áreas de Acceso Informático Restringido deberán mantener un registro foliado correlativamente, de los accesos a los sitios bajo su responsabilidad en el que se identifique al menos el nombre de las personas autorizadas para su ingreso, la fecha y hora de entrada y salida, y de los equipos electrónicos: de cómputo, de almacenamiento, de comunicaciones, de accesorios y otros dispositivos que hayan ingresado y los motivos para su ingreso.

11.- Los responsables del control de acceso a las Áreas de Acceso Informático Restringido se encargarán de vigilar que se realicen las acciones para mantener las condiciones físicas y ambientales necesarias para proteger adecuadamente los recursos informáticos y la información electrónica que contengan.

12.- La Gerencia de informática en conjunto con el responsable del Activo Fijo de la Gerencia Administrativa, serán responsables de vigilar que los bienes de cómputo y comunicaciones de su Unidad Administrativa que no se encuentren en uso sean ubicados en lugares físicos con las condiciones adecuadas para minimizar las posibilidades de sustracción, daño y deterioro

13.- El Jefe de Red y Soporte a Usuarios debe verificar que los respaldos de información electrónica sensible se realicen bajo las condiciones de Seguridad Informática que se encuentren vigentes.

14.- Todo sistema de aplicación sensible a pérdidas potenciales y que requieran un tratamiento especial deben ejecutarse en una computadora dedicada (aislada) que solo debe compartir recursos con sistemas de aplicación confiable.

15.-Todo equipo de cómputo que lleve un registro de eventos debe mantener una sincronización de su reloj a de fin garantizar la exactitud de los registros de auditoría.

16.- Los Sistemas Multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

17.- Toda aplicación que transmita información clasificada fuera de la Institución debe manejar la información cifrada.

18.- Todo el equipamiento que se utilice para generar, almacenar y archivar claves debe ser considerado crítico y de alto riesgo.

19.- Para evitar exponer información utilizando algunos canales ocultos y código malicioso de medios indirectos el Responsable de la Seguridad Informática debe:

a. Adquirir programas a proveedores acreditados o productos debidamente evaluados.
b. Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
c. Controlar el acceso y las modificaciones al código instalado.
d. Utilizar herramientas para la protección contra la infección del software con código malicioso.

20.- Para todo desarrollo de software realizado por terceros se deben establecer:

a. Acuerdos de licencias, propiedad de código y derechos conferidos;
b. Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de quien proporciona el servicio;
c. Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso,
d. verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.;

e. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías, y;
f. Verificar el cumplimiento de las condiciones de seguridad contempladas.
g. Todo plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo.

E.- Seguridad de los Servicios Informáticos de la SIGET.-

1.- Los responsables de servicios informáticos deberán mantener actualizados, configurados y en operación los equipos, accesorios y software relacionado con sus servicios atendiendo las recomendaciones de los fabricantes, proveedores e indicaciones de la Gerencia de Informática.

2.- Los responsables de servicio informáticos serán encargados de:

a) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales como: robo o hurto, incendio, explosivos, humo, inundaciones o filtraciones de agua (o falta de suministro, polvo, vibraciones, efectos químicos, interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión), radiación electromagnética, derrumbes, etc.;

b) Administrar las contraseñas de acuerdo al procedimiento de gestión de contraseñas

c) Aislar de las inclemencias ambientales (temperatura, humedad, etc.) los elementos que requieren protección especial para reducir el nivel general de protección requerida;

d) Almacenar la documentación del sistema en forma segura y restringir el acceso a la documentación del sistema al personal autorizado por el Responsable de la Información;

e) Asegurar la disponibilidad del equipo informático mediante un programa permanente de mantenimiento preventivo y correctivo;

f) Asignar los privilegios a los usuarios de acuerdo a la solicitud y aprobación del Enlace Informático y solicitar a intervalos regulares una revisión de derechos de accesos de los usuarios;

g) Atender las medidas y recomendaciones que se acuerden con el responsable de la Seguridad Informática;

h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron su perfil, o de aquellos a los que se les revocó la autorización, se desvincularon de la Institución o sufrieron la pérdida/robo de sus credenciales de acceso previa notificación del Enlace Informático del área de su adscripción;

i) Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar;

j) Controlar el acceso lógico a los servidores, tanto a su uso como a su administración;

k) Documentar y mantener actualizados los procedimientos operativos de los sistemas de Información Electrónica;

l) Efectuar el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados tomando en cuenta los nuevos requerimientos de los sistemas así como las tendencias actuales proyectadas en el procesamiento de la información de la Institución para el período estipulado de la vida útil de cada componente;

m) Efectuar revisiones periódicas de registro de usuarios con el objeto de:

i. Cancelar identificadores y cuentas de usuario redundantes;

ii. Inhabilitar cuentas inactivas de acuerdo a normativa; y

iii. Eliminar cuentas inactivas de acuerdo a normativa

n) En coordinación con el Departamento de Administración de Redes y soporte y el responsable de Seguridad Informática realizar ejercicios de análisis de riesgos a fin de garantizar la continuidad de los servicios y contribuir al Sistema de Seguridad de la Información;

o) Establecer en coordinación con el responsable de Seguridad Informática los procedimientos para asegurar la continuidad operativa y la recuperación del servicio e información en caso de eventualidades o desastres;

p) Establecer los controles de acceso a las aplicaciones, contemplando al menos los siguientes aspectos:

i. Identificar los requerimientos de seguridad de cada una de las aplicaciones.

ii. Identificar toda la Información relacionada con las aplicaciones.

iii. Definir los perfiles de acceso de Usuarios estándar, comunes a cada categoría de puestos de trabajo.

iv. Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles;

q) Establecer medidas para monitorear el funcionamiento del servicio y detectar de manera oportuna aquellos incidentes que pudieran afectar de alguna forma al desempeño, disponibilidad, confiabilidad, entre otros:

i. Identificar los controles de prevención, detección y corrección;

ii. Instalar periódicamente las actualizaciones de seguridad;

iii. Implementar procedimientos para la administración de medios informáticos removibles, considerando:

- Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la Institución.
- Requerir autorización para retirar cualquier medio de la Institución y realizar un control de todos los retiros a fin de mantener un registro de auditoría.

- Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

r) Mantener instalados y habilitados sólo aquellos servicios que sean utilizados;

s) Mantener el registro de los incidentes que hayan afectado de alguna forma al desempeño, disponibilidad, confiabilidad, etc. Identificando al menos: la causa, el ente que lo originó (al mayor nivel de precisión que sea posible), el nivel de gravedad, los alcances, los efectos percibidos, la solución adoptada y las medidas establecidas para minimizar la posibilidad de que vuelva a presentarse;

t) Mantener el registro de los usuarios autorizados para hacer uso del servicio identificando para cada uno de ellos, al menos: la vigencia de la autorización, los permisos y restricciones con respecto al servicio y el estado para su acceso (por ejemplo: activo, cancelado, inactivo, etc.);

u) Mantener restringido y protegido el acceso a la información institucional que sea manejada por el servicio del que son responsables, atendiendo a los lineamientos emitidos por el Comité de Seguridad Informática y a la normatividad que establezca el área responsable de la Seguridad de la Información;

v) Otorgar al usuario los privilegios mínimos necesarios para desarrollar su trabajo, en consecuencia si existiera algún servicio especial para el desarrollo de sus funciones debe de tramitarlo con la Gerencia de Informática.

w) Otorgar el acceso a los recursos, funciones y servicios informáticos sólo hasta que se hayan completado los procedimientos formales de autorización de acuerdo a la normatividad vigente;

x) Registrar, documentar y comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones con la finalidad de que sean utilizadas para tomar medidas correctivas;

y) Registrar las actividades realizadas en la operación de sistemas y servicios informáticos;

z) Registrar y monitorear aquellos eventos que consideren críticos para la operación que se encuentra bajo su responsabilidad;

aa) Revisar los registros de auditoría con la finalidad de producir un informe de las amenazas detectadas contra los sistemas, para realizar un análisis de riesgos.

bb) Ubicar el equipamiento crítico para proporcionar el servicio en las Áreas de Acceso Informático Restringido que sean designadas por la GI;

cc) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas; y

dd) Las demás que determine el Titular de la Gerencia de Informática (GI).

3.- El Responsable de Seguridad de Informática en coordinación con Servicios Generales de la Gerencia Administrativa y el Comité de Seguridad y Salud Ocupacional (COSSO) deben:

a) Garantizar que existan al menos un equipo portátil de combate y extinción de incendios para hacer frente a cualquier eventualidad que se pueda presentar.

b) Contar con el suministro de energía eléctrica interrumpible (UPS) para garantizar la continuidad del servicio a la infraestructura de cómputo y comunicaciones que soporta las operaciones informáticas críticas de la Institución;

c) Verificar la funcionalidad de la planta generadora de energía eléctrica de respaldo para mantener la continuidad del suministro eléctrico en caso de falla o falta de suministro por parte de la compañía encargada de proporcionarla

d) Disponer del suficiente suministro de combustible para garantizar que la planta generadora de energía eléctrica pueda funcionar por un período prolongado;

e) Implementar protección contra descargas eléctricas en todos los edificios y líneas de comunicaciones externas de acuerdo a las disposiciones normativas vigentes,

f) Proporcionar las condiciones de temperatura y humedad relativa en los centros de procesamiento de datos a fin de garantizar el ambiente de Tecnologías Informáticas (TI) adecuado para la operación del equipamiento de cómputo y comunicaciones;

g) Proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía en las áreas de la Gerencia de Informática;

h) Verificar la distribución de tomas de energía eléctrica necesarias así como de líneas de suministro para evitar en la medida de lo posible un único punto de falla en el suministro de energía en las áreas de la Gerencia de Informática;

i) Verificar que las plantas generadoras de energía eléctrica sean inspeccionadas y probadas periódicamente para asegurar que funcionen adecuadamente;

j) Verificar que los equipos de energía interrumpible sean inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que cuentan con el tiempo de respaldo requerido.

4.- El Responsable de Administrar de la Red debe:

a) Controlar que los cambios en los componentes operativos y de comunicaciones no afecten a la seguridad de los mismos ni de la información que soportan;

b) Establecer los criterios de aprobación para nuevos Sistemas de Información, actualizaciones y nuevas versiones del mismo, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva;

c) Evaluar y registrar previamente todo cambio de operaciones en cuanto a aspectos técnicos y de Seguridad Informática, mediante el Procedimiento de Control de Cambios;

d) Evaluar el posible impacto operativo de los cambios previstos y verificar su correcta implementación;

e) Registrar toda la información relevante de cada cambio implementado; y

f) Las demás que determine el Titular de la Gerencia de Informática (GI).

5.- El Jefe de Programación y Desarrollo debe:

a) Administrar todos los programas fuentes;

b) Asegurar que todo programa ejecutable en producción tenga un único programa fuente asociado que garantice su origen;

c) Asegurar que todo cambio a realizar en el software de aplicación debe efectuarse en el ambiente de desarrollo;

d) Asegurar que para cada cambio realizado en el software de aplicación deben actualizarse los respectivos cambios en el manual de usuario y en la documentación operativa;

e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación;

f) Contar con un control que permita determinar las responsabilidades del personal involucrado en el proceso de entrada de datos;

g) Definir Responsables de la Información para cada uno de los ambientes de procesamiento existentes;

h) Definir un procedimiento para que durante la etapa de diseño, se incorporen controles de validación a fin de eliminar los riesgos de fallas de procesamiento y vicios por procesos de errores;

i) Determinar qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados;

j) Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios;

k) Elaborar una evaluación de riesgos antes de diseñar la aplicación con el objeto de definir los requerimientos de seguridad e identificar los controles apropiados a aplicar en las etapas del desarrollo de sistemas, prueba de las aplicaciones y ambiente de producción;

l) Establecer procedimientos para validar la salida de los datos de las aplicaciones;

m) Identificar y documentar claramente la sensibilidad de cada aplicación;

n) Identificar y acordar con el Administrador de la Aplicación sensible cuando deba de ejecutarse en un ambiente compartido y las aplicaciones con las que compartirá los recursos;

o) Impedir el acceso a los compiladores, editores y otras utilerías del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo;

p) Implementar controles que aseguren la validez de los datos introducidos;

q) Incluir controles de seguridad y registros de auditoría con el objeto de evitar la pérdida, modificación o uso inadecuado de los datos en los Sistemas de Información;

r) Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operación; y

s) Llevar un registro actualizado de todos los programas fuentes en uso, indicando el nombre del programa, programador, analista del programa, versión, fecha de última modificación, fecha / hora de compilación y estado (en modificación, en producción)

t) Respaldar en medios seguros las tres últimas versiones de los programas fuente y ejecutables así como su documentación de entorno de cada aplicación como medida de prevención para cualquier contingencia;

u) Restringir el acceso a la información por fuera del sistema para evitar la modificación directa del dato almacenado, la excepción de uso de las aplicaciones para actualización o eliminación de Información Electrónica se debe realizar a través de una solicitud formal previa autorización del Responsable de la Información;

v) Separar las actividades y ambientes de las áreas de desarrollo, pruebas y producción en entornos diferentes;

w) Toda actualización realizada a las aplicaciones debe ser registrada

x) Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los Usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión;

y) Verificar que todo sistema desarrollado e instalado al interior de la Institución y puesto en producción generen registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad;

- ✓ Verificar que los registros de auditoría sean archivados preferentemente en un equipo diferente al que los genere.
- ✓ Verificar que todo cambio a realizar en las aplicaciones sea propuesto por Usuarios autorizados, que tenga la aprobación del Responsable del Sistema de la Información y que no se violen los requerimientos de Seguridad Informática; y
- ✓ Las demás que determine el Titular de la Gerencia de Informática.

6.- El Jefe de Administración de Redes está obligado a:

a) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal;

b) Determinar los requerimientos para resguardar una copia de cada software o dato en función de su criticidad;

c) Disponer y controlar la realización de copias de respaldo;

d) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo; una vez concluida la posibilidad de ser reutilizados y asegurar la destrucción de los medios desechados;

e) Extender los mismos controles de seguridad aplicados a los dispositivos en el sitio principal al sitio de resguardo;

f) Probar periódicamente los sistemas de resguardo, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la Institución;

g) Retener al menos tres generaciones o ciclos de información de resguardo para la información y el software esenciales para la Institución, y

h) Las demás que determine el Titular de la Gerencia de Informática.

7.- El Jefe de Administración de Red debe de:

a) Autenticar las conexión de nodos de los Sistemas Informáticos;

b) Definir procedimientos para solicitar y aprobar accesos a Internet;

c) Establecer un programa de:

c.1 Control de cambios (etiquetado, documentación, control de activos);

c.2 Control de red (diagramas), y

c.3 Mantenimiento.

d) Implementar controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Institución, contra el acceso no autorizado;

e) Implementar controles para limitar la capacidad de los entornos de conexión de los Usuarios:

e.1 Correo electrónico;

e.2 Transferencia de archivos (FTP);

e.3 Acceso interactivo. (Terminal Remota);

e.4 Acceso a la red fuera del horario laboral. (VPN, RAS, etc.),

f) Incorporar controles de ruteo que verifiquen la dirección de origen y destino, para asegurar que las conexiones informáticas y los flujos de información no violen los Controles de Acceso.

g) Proteger el cableado que transporta datos o soporta servicios de información contra posibles intercepciones o daños;

h) Proteger el tendido del cableado troncal (backbone) mediante la utilización de ductos blindados;

i) Proteger las conexiones realizadas en los puertos de diagnóstico y configuración remota;

j) Registrar los accesos de los Usuarios a Internet con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares;

k) Realizar una evaluación de riesgos para la autenticación de usuarios que requieren conexiones externas a la institución;

l) Separar los cables de energía de los cables de comunicaciones para evitar interferencias;

m) Subdividir la red en dominios lógicos separados con el objeto de controlar la seguridad de la red Institucional;

n) Verificar que las áreas en los puntos terminales y de inspección tengan cerradura;

o) Utilizar piso falso, canaleta o cableado oculto en la pared, siempre que sea posible, cuando corresponda a las Instalaciones de Procesamiento de información;

p) Verificar que el cableado cumpla con los requisitos técnicos vigentes de las Normas establecidas; y

q) Las demás que determine el Titular de la Gerencia de Informática.

8.- El Jefe de Administración de Redes debe:

a) Proteger contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.;

b) Proteger los archivos adjuntos de correo electrónico;

c) Usar técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos;

d) Instrumentar controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados;

e) Establecer aspectos operativos para garantizar el correcto funcionamiento del servicio (ejemplo: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del Usuario, etc.);

9.- El Jefe de Administración de Redes en relación con la mensajería electrónica debe:

a) Asegurar que toda actualización que deba realizarse en el sistema operativo debe ser probada en equipos piloto por el Responsable del Servicio Informático a fin de garantizar que no se produzcan impactos negativos en su funcionamiento y Seguridad Informática; Limitar y controlar el uso de utilerías del sistema operativo;

b) Realizar una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo;

c) Utilizar la Norma de Nomenclatura de Equipos de Cómputo y Servidores para la identificación de los equipos de cómputo ubicada en el sitio de normas informáticas en la intranet; y

d) Las demás que determine el Titular de la Gerencia de Informática.

10.- El Jefe de Administración de Redes debe:

a) Controlar el acceso a los archivos del sistema de manera segura; y

b) Las demás que determine el Titular de la Gerencia de Informática.

11.- El Jefe de Programación y Desarrollo debe de:

a) Asegurar que todo programa en producción cuente con sus respectivos manuales.

b) Controlar que no se de mantenimiento de programas en el ambiente de producción;

c) Resguardar todos los programas ejecutables en el ambiente de producción; y

d) Las demás que determine el Titular de la Gerencia de Informática.

12.- El Jefe de Programación y Desarrollo debe:

Realizar las pruebas con una copia de datos extraídos del ambiente operativo y una vez terminada la prueba se debe borrar su contenido.

13.- Las aclaraciones de interpretación de la presente política, deben ser remitidas al Responsable de la Seguridad Informática de SIGET.

14.- El incumplimiento de las disposiciones establecidas en estas Políticas será objeto de sanción administrativa en los términos de la Ley aplicable, independientemente de las sanciones de las que pudieran hacerse acreedores en términos de las demás disposiciones jurídicas aplicables.

SECCION 02

POLÍTICA PARA EL USO DE INTERNET.

Propósito

Establecer los parámetros para el uso de internet como herramienta de trabajo.

Alcance

Aplica para todos los empleados vinculados a la institución, oficina central y centros de atención al usuario de Santa Ana y San Miguel.

Lineamientos

1. El acceso a internet será asignado de acuerdo a los cargos que lo requieran por el desempeño de sus funciones, de acuerdo a la autorización del Gerente o Jefe de Unidad Organizativa.
2. Todos los empleados deberán firmar de conformidad de aceptación y entendimiento de la presente política.

3. De acuerdo a los cargos y responsabilidades administrativas asignadas, se otorgaran permisos especiales para los accesos, siempre con a la autorización del Gerente o Jefe de Unidad Organizativa.

4. Se espera por parte de los empleados un uso adecuado y responsable del Internet, sin embargo, la utilización para fines personales con efectos en los niveles no autorizados tendrá sanciones disciplinarias.

5. No se permite el acceso a sitios web para adultos, música, juegos, hacking, videos, streaming, compras en línea, etc.

6. Es prohibido realizar descargas de software o similar, sin la autorización previa del Superintendente, previo aval del Gerente o Jefe de Unidad Asesora.

7. El acceso a redes de otras organizaciones o compañías debe ser avalado por el Superintendente.

8. El acceso a páginas o vídeos especializados debe ser autorizado por el Superintendente, previa justificación de las razones de acceso con el desarrollo de las funciones por el Gerente o Jefe de Unidad Asesora.

9. Es deber de todos los empleados mantener la configuración del navegador de internet asignado por la organización. Cualquier cambio sin la autorización del Superintendente genera acciones disciplinarias.

10. Es responsabilidad del Jefe de Programación y Desarrollo actualizar el navegador de internet, de acuerdo a las necesidades de los sistemas.

11. La Gerencia de Informática se reserva el derecho de auditar las acciones ejecutadas en la red por cualquier empleado y sus resultados deben ser reportados al Superintendente.

12. Las aclaraciones de interpretación de la presente política, deben ser remitidas al Responsable de la Seguridad Informática de SIGET.

13. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCION 03

POLÍTICA PARA EL USO DE REDES SOCIALES.

Definición de Redes Sociales

"El término red, proviene del latín rete, y se utiliza para definir a una estructura que tiene un determinado patrón. Existen diversos tipos de redes: informáticas, eléctricas, sociales. Las redes sociales se podrían definir como estructuras en donde muchas personas mantienen diferentes tipos de relaciones amistosas, laborales, amorosas.
Por lo tanto hoy en día el término "red social " se llama así a los diferentes sitios o páginas de internet que ofrecen registrarse a las personas y contactarse con infinidad de individuos a fin de compartir contenidos, interactuar y crear comunidades sobre intereses similares: trabajo, lecturas, juegos, amistad, relaciones amorosas, entre otros."

De acuerdo a lo que plantea Jaime Royero (2007) define las redes sociales como "el conjunto de personas, comunidades, entes u organizaciones que producen, reciben e intercambian bienes o servicios sociales para su sostenimiento en un esquema de desarrollo y bienestar esperado. Dicho bienestar es mediatizado por los avances en el campo de la ciencia y la tecnología producidos y ofrecidos en su valor social y mercantil a las personas o grupos de ellas, en un territorio y en unas condiciones económicas sociales determinadas. Estos intercambios se dan a nivel local regional, nacional, internacional y global".[1]

[1] http://www.monografias.com/trabajos84/redes-sociales/redes-sociales.

Propósito

Establecer los parámetros para el uso de las redes sociales en la institución, pues se considera que las mismas deben ser utilizadas como una herramienta de apoyo, para lo cual se invita a todos los empleados al buen uso de las mismas.

Alcance

Aplica para todos los empleados de la SIGET, incluyendo los Centros de Atención al Usuario de Santa Ana y San Miguel.

Principios

Los principios de nuestra institución deben ser la base para la actividad en las redes sociales, por lo cual se espera que todos nuestros empleados las consideren antes de realizar cualquier publicación:

a. Cumplir con el Código de Ética Gubernamental. Todas las publicaciones realizadas deben ser verificadas antes de su divulgación, validando que se ajusten al Código de Ética y a la presente Política.

b. Privacidad. Toda la información que se comparta en las redes debe estar expresamente autorizada para dicha divulgación, por lo cual nunca se podrá compartir información confidencial de nuestra institución, usuarios, operadores, clientes y proveedores.

c. Transparencia. Para las cuentas institucionales, los usuarios, operadores, clientes y proveedores deben conocer expresamente el nombre del funcionario con el cual mantienen contacto, así como la información entregada debe ser la autorizada por la Institución. En ningún caso se permite la manipulación de la información;

d. Informar. Todos los colaboradores debemos informar al Departamento de Comunicaciones y Relaciones Públicas, cualquier situación que no corresponda con la de la institución o que atente con nuestro buen nombre.

Lineamientos

1. El responsable de administrar las redes sociales de SIGET es el Departamento de Comunicaciones y Relaciones Públicas.

2. Ningún empleado de la SIGET, podrá realizar publicaciones de la institución en sus cuentas personales de información confidencial o privada, así como de compañeros de trabajo (Estrategias, lanzamientos, resultados institucionales o financieros, regulaciones, usuarios, operadores, clientes, proveedores y demás temas).

3. Todos los empleados de SIGET deben propender por mantener el bueno nombre y la imagen tanto personal como de la institución, por lo cual sus publicaciones deben ser respetuosas, proyectando los principios y valores de la SIGET.

4. Es prohibido utilizar los equipos de la SIGET para el uso de las cuentas personales en redes sociales, así como de realizar publicaciones en el horario laboral.

5. Solo si la institución lo autoriza expresamente, se puede utilizar la imagen de la SIGET, para lo cual el Departamento de Comunicaciones y Relaciones Públicas, informará las instrucciones correspondientes para su uso a todos los empleados.

6. Cualquier publicación que realice un empleado que atente contra el buen nombre de la SIGET o de sus compañeros, puede ser considerado como una falta grave, que inclusive puede llevar a su desvinculación de la institución.

7. Todos los empleados vinculados deberán suscribir la aceptación expresa de la presente política, junto con la Ley de Ética Gubernamental.

8. Cualquier equivocación o error en la publicación de las redes sociales, debe ser inmediatamente informada al Departamento de Comunicaciones y Relaciones Públicas, así como los mensajes que afectan el nombre de la institución.

9. Los empleados deben mantener controles de acceso a su información personal y a la de la institución en las cuentas que administran.

10. Cada publicación debe considerar una interpretación global, pues si se hace con un enfoque local, es posible entrar en conflictos de interpretación, de acuerdo a la interpretación de cada cultura.

11. Las aclaraciones de interpretación de la presente política, deben ser remitidas al Responsable de la Seguridad de la Información de SIGET.
12. La Gerencia de Informática se reserva el derecho de auditar las acciones ejecutadas en la red por cualquier empleado y sus resultados deben ser reportados al Superintendente.
13. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCION 04

POLÍTICA PARA EL USO DE APARATOS DE TELEFONIA MOVIL.

Propósito

Establecer los lineamientos para la asignación de teléfonos celulares institucionales y la utilización de los mismos, así como de los celulares personales, durante el horario laboral.

Alcance

Aplica a todos los empleados de la SIGET tanto de la Oficina Central como de los Centros de Atención al Usuario de Santa Ana y San Miguel a los cuales les ha sido asignado el celular de la institución, así como para todos los empleados que usan el celular personal en el horario laboral.

Lineamientos

1. La Gerencia o Jefatura de cada unidad organizativa, deberá aprobar la asignación de celular institucional para los cargos de su área, siempre que se demuestre que dicho colaborador debe desplazarse de las instalaciones de la organización o que debe mantener contacto directo con usuarios, operadores, clientes y proveedores de la SIGET.
2. El Superintendente por medio de la Gerencia Administrativa, es el responsable de solicitar la adquisición de los servicios telefónicos y de la elaboración de los términos de referencias, aprobará la gama de celulares asignados a cada nivel de la SIGET, de tal forma que los mismos cumplan con los requerimientos tecnológicos, así como con los planes de voz y datos que cada cargo requiere.

3. El Superintendente por medio del Administrador del Contrato de los servicios de telefonía fijos y móviles, evaluará los servicios y tarifas ofrecidos por el operador anualmente, de tal forma que se mantenga la mejor opción para la organización frente al mercado.
4. Sin excepción alguna, los contratos que respaldan los servicios de telefonía fija y móvil deberán suscribirse a un plazo no mayor a un año.
5. La Gerencia Administrativa es la responsable de administrar y asignar los celulares institucionales, previa solicitud de la Gerencia o Unidad Asesora, aprobada por el Superintendente.
6. La Gerencia de Informática, es la responsable de parametrizar en cada móvil el correo electrónico del colaborador al cual le ha sido asignado el celular, según previa solicitud de la Gerencia o Jefatura correspondiente.
7. Todo empleado deberá asignar a su dispositivo móvil una clave de ingreso, así como deberá reportar tanto al operador como a la Gerencia la pérdida o robo del celular.
8. Cada empleado es responsable del buen uso del dispositivo entregado, razón por la cual el daño del mismo por su mala utilización debe ser asumido por el empleado.
9. La Gerencia Administrativa podrá solicitar la realización de auditorías para validar el buen uso de los celulares asignados por la SIGET, y por tanto podrá implementar las acciones correctivas que considere.
10. El equipo que no sea entregado al momento del retiro del empleado, será descontado de su correspondiente liquidación.
11. Los empleado que se desplacen en vehículo y deben atender una llamada laboral, deberán cumplir con las normas de tránsito y por tanto deberán hacer uso del manos libres.
12. Durante las reuniones de trabajo se espera que los participantes asignen el estado de "reunión", de tal forma que la misma no sea interrumpida.

En caso de ser imprescindible atender la llamada, los participantes deberán informar a los demás miembros.

13. El valor del límite de consumo de telefonía celular por empleado en el mes, deberá establecerse mediante acuerdo administrativo, definiendo en el mismo además que el exceso del consumo sobre el límite establecido será cobrado al empleado por medio de descuento en planilla.
14. Cualquier duda de interpretación de la presente política debe ser resuelta por El Encargado del Área de Seguridad.
15. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 05

POLÍTICA PARA LA ADMINISTRACION DE LAS CLAVES.

Propósito

Establecer los lineamientos para la creación, administración y modificación de claves en los diferentes sistemas en los cuales la organización apoya su operación, brindando seguridad y por tanto reduciendo el riesgo de accesos no autorizados.

Alcance

Involucra a todo el personal de la organización que tiene acceso personalizado a cualquiera de los sistemas y/o cuentas electrónicas de SIGET, tanto en la Oficina Central como en los Centros de Atención al Usuario ubicados en Santa Ana y San Miguel.

Lineamientos

1. Cada usuario siempre deberá contar con su clave y en ningún caso se permite que la misma sea compartida con otro empleado, siendo responsabilidad única del titular las operaciones y transacciones que se registren a su nombre.
2. Los usuarios que tengan por su cargo la responsabilidad de administrar una clave, deberán asignarlo considerando que el mismo sea de fácil recordación pero que a la vez no sea de fácil identificación, por lo cual no podrán ser nombres de familiares, hijos, mascotas, fechas especiales o palabras comunes.
3. Las claves deberán cumplir con las siguientes características:
   a. Caracteres en mayúsculas
   b. Caracteres en minúsculas
   c. Números

d. Signos de puntación

e. Caracteres tales como @, $, &, (), +,-, $

f. Deben estar compuesto por al menos seis caracteres.

4. Las claves no pueden estar compuestos por palabras o números tales como 1234 o *aaaa o bbbbb*.
5. Las claves deben ser cambiados al menos cada mes.
6. No se permiten los usuarios ni las claves genéricas en ningún sistema de la organización.
7. Se deben utilizar diferentes claves para cada uno de los sistemas o cuentas asignadas al colaborador.
8. Todos los colaboradores de SIGET no podrán divulgar, escribir o comentar información relacionada con las claves.
9. Nunca se podrá habilitar la opción "recordar contraseña".
10. La Gerencia de Informática, por medio del Departamento de Administración de Redes, es la encargada de administrar los casos de pérdida o divulgación inadecuada de las claves.
11. Toda aplicación que sea desarrollada, deberá considerar los siguientes aspectos en las claves:

    a. Registro por un único usuario

    b. No debe almacenar las contraseñas en cuadernos, PC, etc.

    c. Restringir el acceso a los Sistemas de acuerdo a los permisos y funciones de cada cargo.
12. Los dispositivos móviles deberán tener habilitada la opción de bloqueo y contraseña.
13. Para aquellos sistemas que requieren el uso de *Token* para su acceso, los mismos deben ser custodiados en cajas de seguridad o bajo llave cuando no se estén utilizando.

14. Para todo colaborador que se retire a vacaciones o por incapacidad de la institución, el Departamento de Recursos Humanos es responsable de comunicar a la Gerencia de Informática, para bloquear su usuario, hasta tanto no regrese de sus vacaciones o incapacidad.
15. El Departamento de Recursos Humanos deberá informar o la Gerencia de Informática, las vacaciones, incapacidades y/o ausencias para la actualización de claves.
16. Queda terminantemente prohibido el préstamo de usuarios y claves entre empleados de SIGET.
17. El uso inadecuado de las claves puede llegar a representar una causal de despido con justa causa para los colaboradores de la organización.
18. Cualquier duda de interpretación de la presente política debe ser resuelta por El Encargado del Área de Seguridad Informática.
19. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 06

POLÍTICA PARA LA GESTION DE CAMBIOS EN TECNOLOGIAS DE INFORMACION Y COMUNICACION.

Propósito

Definir los lineamientos para la realización y/o gestión de los cambios en software, hardware, definiendo tanto el método como el procedimiento a seguir para realizar el cambio, reduciendo los riesgos de pérdida o daño de información, así como de afectación en la continuidad de las actividades institucionales.

Alcance

Aplica para la realización de pruebas, revisiones, cambios e implementación de Hardware y Software, así como considera el estudio, aprobación, y puesta en marcha de los cambios.

Lineamientos

1. Es responsabilidad de la Gerencia de Informática definir los procedimientos a seguir tanto para la solicitud como la realización y aprobación de los cambios de Tecnología de Información, especificando las responsabilidades de cada nivel y área.
2. El equipo de cambios en la organización, estará conformado por:
   a. Gerente de la Gerencia de Informática
   b. Gerente o Jefe responsable del Área sujeta de los cambios
   c. Jefe de Administración de Redes
   d. Jefe de Seguridad Informática
   e. Jefe de Programación y Desarrollo

3. Todos los cambios deben ser aprobados formalmente tanto por Gerente de la Gerencia de Informática como por el Gerente o Jefe del Área a la cual corresponde el cambio, según previa documentación soporte de cambios y de acuerdo con la aceptación de los resultados de las pruebas de los cambios realizados.
4. El procedimiento de cambios deberá incluir, los siguientes aspectos:
   a. Clase de cambios
   b. Criterios para clasificar si es un cambio es urgente o puede ser programado
   c. Sustentación técnica y operativa para realizar el cambio.
   d. Evaluación de impacto
   e. Niveles autorizadores del cambio
   f. Pruebas de aceptación
   g. Documentación de los cambios
   h. Responsabilidades del personal de la Gerencia de Informática.
5. Todos los cambios solicitados deben contar con la correspondiente evaluación de riesgos, incluyendo el impacto en la operación, así como su factibilidad técnica, económica y operativa.
6. Todos los cambios que se consideren sean de alto impacto, deben ser aprobados por el Gerente o Jefe del Área Usuaria.
7. Todos los cambios con impacto financiero, deber ser aprobados adicionalmente por el Gerente de la Gerencia Financiera.
8. Se consideran cambios urgentes, todos aquellos cambios que no siguen el proceso normal de aprobación, dado que no ejecutarlos en el menor tiempo posible, tiene un impacto negativo en la prestación del servicio, la operación normal de la SIGET.
9. Todo cambio con clasificación de urgencia debe ser reportado y aprobado por el Superintendente.

10. Los cambios, siempre deberán ser realizados primero en el ambiente de pruebas, donde es obligatorio verificar sus niveles de seguridad, así como el que los mismos se ejecutaron de acuerdo a la solicitud y aprobación, sin tener un alcance mayor y/o menor al inicialmente programado.
11. Todos los cambios y/o actualizaciones de software deben tener un control de versiones, así como las versiones anteriores deben mantenerse, facilitando el entendimiento de la naturaleza del cambio y los históricos de los mismos.
12. Los desarrolladores no pueden tener acceso al ambiente real y/o de producción, su acceso debe limitarse únicamente al ambiente de pruebas.
13. Tanto en el ambiente de pruebas como de producción, los ingenieros y técnicos deberán contar con un usuario y clave de acceso, la cual no podrá ser compartida, así como ningún área podrá tener usuarios genéricos.
14. Todos los cambios deben ser informados oficialmente a los usuarios que tienen relación alguna con ellos, así como se deberá considerar un plan de capacitaciones en el mismo, según rubro presupuestal para el plan de formación.
15. Los cambios claves dentro de una herramienta, deben ser considerados como un proyecto y por tanto se debe considerar como una implementación del sistema, siendo responsabilidad del Encargado de Desarrollo, en coordinación con el Jefe de Redes, la realización de su ejecución.
16. Todos los cambios implementados en el ambiente de producción, deben ser monitoreados, reportando oportunamente por parte de El Programador las desviaciones que se pudieran presentar.
17. Los cambios desarrollados que no presenten los resultados esperados, deben ser documentados.

18. Mensualmente, cada programador debe realizar un reporte de los cambios realizados, de acuerdo a su clasificación e impacto, así como debe especificar los inconvenientes presentados por los cambios generados y los cambios programados para el mes siguiente.

19. Cualquier duda de interpretación de la presente política debe ser resuelta por El Jefe de Programación y Desarrollo.

20. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 07

POLÍTICA PARA LA ASIGNACION Y RETIRO DE USUARIOS EN LOS SISTEMAS.

Objetivo

Establecer las directrices bajo las cuales se orienta la creación, administración y retiro de los correspondientes perfiles y usuarios en cada uno de los aplicativos que soportan la operación de SIGET.

Alcance

Aplica para Oficina Central y los Centros de Atención a los Usuarios de Santa Ana y San Salvador, así como para todos los sistemas de información que soportan la operación. Su implementación será inmediata y obligatoria a partir de la fecha de publicación de la misma, razón por la cual los procedimientos existentes deberán ser revisados y ajustados a los lineamientos dados.

Lineamientos

1 Todo empleado o funcionario vinculado a SIGET, se le deberá asignar un usuario único que le permita acceder a cada uno de los sistemas y/o herramientas tecnológicas cuando se requiera para el desarrollo de sus funciones;

2 La autorización para la creación de usuarios y la asignación de su perfil en cada aplicativo, será por medio un requerimiento formal de los Gerentes o Jefes de Área. Para todos los empleados o funcionarios que son vinculados por primera vez a SIGET.

3 El Gerente o Jefe de Área es responsable de validar el perfil asignado al colaborador vinculado, corresponde a las funciones que realizará y en los aplicativos que requiere para su desempeño.

4 La creación de usuarios y la asignación del perfil que corresponda, es realizada por la Gerencia de Informática, según el requerimiento realizado.

5 La Gerencia de Informática es responsable de verificar la disponibilidad de licencias con que cuenta cada aplicativo para la correspondiente creación de usuarios.

6 La asignación del perfil de cada usuario debe garantizar la adecuada segregación de funciones, así como asegurar que el acceso otorgado es acorde al rol que desempeñará

7 No se autorizará la creación de usuarios genéricos.

8 El Gerente o Jefe de Área es responsable de informar el retiro de los empleados o funcionarios a la Gerencia de Informática, garantizando así la oportuna actualización de usuarios.

9 Cualquier duda de interpretación de la presente política debe ser resuelta por el Gerente de la Gerencia de Informática.

10 El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 08

POLITICA PARA LA SEGURIDAD DE LA INFORMACION.

Propósito

Establecer los parámetros para realizar las copias de seguridad de la información en cada uno de los equipos de la organización, así como la restauración de dichas copias, propendiendo por mantener los datos protegidos contra la pérdida o daño, accidental o intencional, permitiendo contar con la información ante cualquier evento que afecte la integridad o completitud de la información.

Alcance

Aplica para todos los equipos e información de la organización que son administrados por el área de Tecnología de Información, tanto de las oficinas principales ubicadas en San Salvador, como las oficinas de Santa Ana y San Miguel.

Conceptos

a) Copias de seguridad: Se copian los datos originales, el cual se realiza con el fin de disponer de un medio para recuperarlos en caso de una pérdida.

b) Restauración: Funciona para cuando en una máquina haya una pérdida total de la información y con la copia de seguridad se pueda restaurar a la fecha de la realización del backup.

c) Copia completa: Copia la totalidad de los datos en otro juego de soportes, que puede consistir en cintas, discos, o en un DVD o CD.

d) Copia parcial: Es una copia de seguridad diseñada para usarse en un modelo de recuperación simple con el de poder mejorar la flexibilidad.

e) Copia Incremental: Esta copia de seguridad solo copiara los datos que hayan cambiado desde la copia anterior.

Lineamientos

1. Las copias de seguridad deben realizarse de acuerdo a lo establecido en el Procedimiento de Recuperación de Servidores.

2. Las aplicaciones críticas serán respaldadas en un sitio alterno de contingencia, según lo establecido en el Plan de Contingencia Informática de SIGET.
3. Las claves de usuario NO serán respaldadas, siempre y cuando no estén encriptados.

4. Es responsabilidad del área de Redes y Soporte a Usuarios realizar las copias de seguridad.

5. Las copias de seguridad deberán ser realizadas para los siguientes datos:
   a. Bases de Datos
   b. Carpetas con información laboral
   c. Copias de Sistemas

6. Las copias de seguridad deberán incluir sin excepción alguna, especificar la siguiente información:
   a. Usuario
   b. Nombre del sistema
   c. Fecha de creación
   d. Clasificación de la información contenida.

7. Las copias de seguridad deben ser realizadas en las noches, sin afectar la operación de la organización.
8. En caso de requerir realizarlo en el día, dicha actividad debe ser autorizada por Gerente/Jefe de la Unidad a la que se le hará la copia de seguridad.
9. Las rutinas de las copias de seguridad debe ser diseñadas de tal forma que no requieran la intervención manual.
10. La seguridad y custodia de la información almacenada en equipos portátiles, es responsabilidad de cada uno de los usuarios asignados.
11. Las oficinas que no se encuentran en la red institucional, deberán tener un procedimiento para la realización de sus copias de seguridad, las cuales deberán enviar a la Gerencia de Informática, cada mes, por medio de CD o con soporte de la Gerencia de Informática.
12. Las copias de seguridad deben ser custodiadas en servidores externos y remotos a la ubicación geográfica de la organización o en la nube, facilitando su recuperación ante un desastre.
13. El acceso a las copias de seguridad deberá ser aprobado por el Área de Seguridad, quien periódicamente revisará dichos accesos. El número de usuarios con acceso a dichas copias deberá ser entre 2 y 5 colaboradores máximo.
14. Es responsabilidad del área de Redes y Soporte a Usuarios verificar la correcta ejecución de las copias de seguridad.
15. Los log de cada respaldo deberán quedar registrados en la máquina donde son realizados (logs de servidor) y en un archivo externo (texto, planilla, etc.) que permita dejarlo disponible para controles o auditoría.
16. Cada tres meses, se deberán ejecutar y documentar las pruebas de restauración de las copias de seguridad por parte del Encargado de la Seguridad, con apoyo del Jefe de Administración de Red.

17. En el caso de que un usuario solicite la restauración o recuperación de una copia de seguridad, esta deber ser autorizada por su Jefe Inmediato, la Gerencia del Área o Jefatura de Unidad y el Superintendente.

18. La presente política debe estar alineada con el plan de contingencia establecido por SIGET, siendo un complemento de la misma, así como debe ser revisada y actualizada anualmente, considerando la inclusión de nuevas tecnologías.

19. Cualquier duda de interpretación de la presente política debe ser resuelta por El Encargado de la Seguridad de la Información.

20. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 09

POLÍTICA DE ADMINISTRACIÓN Y USO DE SOFTWARE.

Propósito

Establecer los lineamientos tanto para la adquisición, utilización, mantenimiento, formación y retiro de todo software requerido para la operación de la organización, propendiendo por el cumplimiento de la legislación nacional e internacional con relación al uso de software legal y por tanto la protección de los derechos de autor.

Alcance

La presente política debe ser aplicada en Oficina Central como en las Unidades de Atención al Usuario ubicadas en Santa Ana y San Miguel, y debe darle cumplimiento cada usuario desde su rol. La política aplica para todos aquellos equipos que son propiedad de SIGET tales como servidores, computadores de escritorio, portátiles, tabletas, celulares, etc.

Conceptos

a) *Usuario:* Son todos aquellos colaboradores, proveedores y clientes que de acuerdo a su rol, deben utilizar las diferentes aplicaciones de software que soportan la operación de la organización.

b) *Licencia de Software*: Se entiende por licencia de software todo aquel contrato suscrito con el representante que tiene los derechos sobre el mismo, y el cual autoriza el uso de dicho software a la organización, incluyendo plazos y usos permitidos.

c) *Tipos de Software*: Según las condiciones de uso, el mismo se puede clasificar en:

i) Licenciado: Aplicación que permite a los usuarios una o varias tareas específicas.

ii) Libre: El propietario de dicho software permite su utilización a todo usuario que lo requiera, sin que por su uso se deba dar alguna contraprestación económica.

Lineamientos

1. SIGET deberá mantener en todos sus equipos (*servidores, computadores de escritorio, portátiles, tabletas, etc.)* aplicaciones de software legal, dando cumplimiento a la protección de los derechos de autor.
2. SIGET no permite ni acepta bajo ninguna circunstancia el uso de software no legal.
3. Todos los usuarios de la organización, tienen prohibida la copia o la utilización no autorizada de aplicaciones de software de SIGET, sin haber sido autorizados por El Superintendente.
4. Es deber de todos los empleados, utilizar el software de acuerdo a las condiciones y parámetros de la licencia otorgada por el dueño del mismo.
5. La utilización de software no legal en los equipos de la organización o la reproducción no autorizada del software legal, puede ser considerada como justa causa para el despido, previa investigación realizada por el área de Auditoría Interna y de la Gerencia de Informática, así como *puede* dar inicio a las investigaciones legales por parte de las autoridades competentes.
6. Es responsabilidad del área de Desarrollo y Programación, mantener actualizadas y vigentes las licencias de software con las cuales trabaja la SIGET.
7. Todo software adquirido debe tener en sus registros el área en la cual es utilizado.

8. Tanto la compra de software como la capacitación que debe brindarse a los empleados de la organización, debe contar con una partida presupuestal anual y la cual es responsabilidad de la Gerencia de Informática.

9. El cambio de versión de una aplicación de software, deberá estar sustentada técnica y financieramente por el Área de desarrollo o programación, así como deberá considerar la calificación anual del proveedor, los riesgos de la actualización, la continuidad de la operación y el soporte del proveedor, entre otros factores.

10. La compra o alquiler de software en relación a características técnicas es responsabilidad de la Gerencia de Informática y únicamente se podrá realizar con proveedores reconocidas y registrados legalmente.

11. Ningún área diferente a la Gerencia de Informática podrá realizar la gestión de compra o alquiler de software. En caso que un área requiera un software especializado o su actualización, deberá solicitarlo a la Jefatura de la Gerencia de Informática, por medio de nota explicativa.

12. El Departamento de Recursos Humanos es la responsable de liderar las jornadas de capacitación tanto para los colaboradores nuevos como para todos aquellos que lo requieran al momento de realizar actualizaciones o adquirir nuevas herramientas.

13. Los empleados del área de la Gerencia de Informática, según las responsabilidades de sus cargos, son los únicos autorizados para instalar o retirar el software adquirido por la organización.

14. No es permitido que los empleados de la organización realicen descargas de herramientas que no tienen la correspondiente autorización del Superintendente.

15. Es responsabilidad de la Gerencia de Informática, garantizar que la organización cuente con un software antivirus, así como el que el mismo se actualice en cada uno de los equipos de la organización.

16. Todo empleado de SIGET que recibe equipos de cómputo, debe suscribir la declaración de aceptación y entendimiento de la presente política.

17. Es deber de todos los empleados informar o denunciar el uso de software no legal, así como la copia no autorizada de los programas de la organización.

18. Cualquier duda de interpretación de la presente política debe ser resuelta por El Encargado de la Seguridad de la Información.

19. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 10

POLITICA DE CONFIDENCIALIDAD.

Propósito

Establecer los lineamientos bajo los cuales se debe manejar la información de SIGET, tanto en Oficina Central como en los Centros de Atención a los Usuarios habilitados en Santa Ana y San Miguel, por parte de cada uno de los miembros de la institución, protegiendo la información así como su divulgación no autorizada a terceros que pueda poner en riesgo a la entidad.

Alcance

Aplica a todos los empleados vinculados con SIGET tanto de Oficina Central como de los Centros de Atención a los Usuarios habilitados en Santa Ana y San Miguel. Su aplicación será inmediata y obligatoria a partir de la fecha de publicación de la misma.

Lineamientos

1. Toda la información de la organización debe ser utilizada únicamente para los fines de la organización.
2. Cada empleado es responsable de la custodia y adecuado manejo de la información a la que tiene acceso para el cumplimiento de sus funciones.
3. La custodia, niveles de acceso y entrega controlada de la información clasificada con categoría de confidencialidad alta y acceso restringido será responsabilidad de las Gerencias y Jefaturas de la institución.

4. La divulgación de la información clasificada como altamente confidencial y con acceso restringido, será compartida por El Superintendente de SIGET únicamente a los empleados que por el desempeño de sus funciones deben conocerlos, y para lo cual dichos documentos deberán contar con claves de acceso y tener la marca "confidencial" o "privado".

5. La divulgación de la información privilegiada deberá contar con la autorización del Superintendente.

6. Todo documento clasificado como altamente confidencial, deberá contar con copias controladas, de tal forma que se tengan registros de los empleados que cuentan con dicha información, así como la fecha de entrega y el fin para el cual se realizó su entrega.

7. Todos los empleados deberán suscribir un acuerdo de confidencialidad o no divulgación.

8. Se considera información privilegiada lo siguiente:

   a. Información financiera.

   b. Planes de Asociación y Expansión.

   c. Estrategias de crecimiento y cambios de estructura en la institución.

   d. Planes estratégicos y operativos.

   e. Información de investigación y desarrollo de asignación de frecuencias.

   f. Información personal de los servidores y funcionarios Públicos de SIGET.

   g. Información relacionada con resoluciones y apelaciones.

   h. Información de Usuarios, Operadores, Clientes y Proveedores.

9. Se considera una falta grave la divulgación o manejo inadecuado de la información de SIGET, generando procesos disciplinarios internos o judiciales, por los daños o perjuicios causados.

10. Todo empleado de SIGET tiene el deber de informar cualquier situación que afecte la confidencialidad de la información.

11. Los miembros de la Unidad de Auditoría Interna tendrán acceso a la información que requieran para el desarrollo de sus labores.

12. Se deberán contar con copias de seguridad de la información.

13. Todo empleado deberá cumplir con los siguientes protocolos en su puesto de trabajo

    a. Antes de retirarse de su equipo de cómputo, el mismo deberá quedar bloqueado

    b. Los documentos de trabajo deberán ser guardados bajo llave después de terminada su utilización.

    c. Al terminar su trabajo en un aplicativo se debe cerrar la sesión.

    d. No podrá prestar su usuario y clave a sus compañeros.

    e. Todo equipo portátil deberá ser asegurado con los elementos entregados por la organización.

    f. Se deben realizar las correspondientes copias de respaldo en el plazo estipulado para ese efecto.

    g. Todo empleado debe propender por ser cuidadoso en realizar comentarios inadecuados o de información privilegiada de la organización en reuniones sociales y/o familiares.

14. El Centro de Datos deberá contar con al menos los siguientes elementos:

- Puertas de seguridad
- Cámaras
- Alarmas
- Registros de acceso

15. Todos los contratos que suscriba SIGET con proveedores, sean estos personas naturales o jurídicas, en los cuales se revele información catalogada como confidencial por parte de la institución, deberán incluirse cláusulas de confidencialidad en dichos contratos. Se entiende que toda la información que proporcione SIGET por cualquier medio a la parte receptora es de carácter confidencial, salvo las excepciones que expresamente estén contenidas en el contrato.

16. Cualquier duda de interpretación de la presente política debe ser resuelta por El Encargado de la Seguridad de la Información.

17. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 11

POLITICA PARA LA ADMINISTRACION DEL DATA CENTER.

Propósito

Establecer los lineamientos para una administración segura y eficiente del Data Center; considerando el esquema organizacional, seguridad, ubicación y acceso a las instalaciones, visitas al centro de datos, protección contra siniestros, esquema de mantenimientos de los equipos y capacitación en procedimientos de seguridad del personal responsable del Data Center.

Alcance

La presente política debe ser aplicada en todas las Oficina Centrales de San Salvador y en los Centros de Atención al Usuario de Santa Ana y San Miguel y debe darle cumplimiento cada usuario desde su rol. La política aplica para todos aquellos equipos que son propiedad de la institución tales como servidores, equipo de enfriamiento, comunicaciones, switches, firewall, E1, etc.

Lineamientos

1. Dentro de la organización debe existir un Área Responsable de la administración de la seguridad e información.

2. Las responsabilidades relativas a la seguridad física y lógica deben encontrarse debidamente asignadas.

3. Deben existir procedimientos dirigidos a garantizar la seguridad de los activos del Data Center (Equipo, Software, Hardware e información) y estos deben definir claramente las responsabilidades de los usuarios, administradores y personal en general.

4. La ubicación del Data Center debe ser la adecuada para proteger la integridad de los activos (equipo, software, hardware e información), debe tener ubicación física segura, de preferencia en el centro de la construcción, no cerca de las paredes exteriores, ni en el sótano, ni último piso.

5. Debe evitarse en lo posible accesos a las instalaciones distintas a la puerta principal. El acceso principal debe estar restringido por el uso de llaves, tarjetas u otros dispositivos de seguridad. Si se usa una clave o cualquier otro medio que active un código interno, este debe cambiarse por lo menos una vez al mes.

6. Abstenerse de colocar señales exteriores que indiquen la ubicación del Data Center a extraños; así como evitar colocar información en los directorios telefónicos y documentación emitida por la Institución.

7. Todos los puntos de entrada y salida del Data Center deben estar equipados con mecanismos de control de acceso. Debe restringirse el acceso al área solo al personal autorizado, para ese efecto es necesario crear una lista de personal autorizado a ingresar al Data Center.

8. Debe llevarse una bitácora por lo menos empastada y foliada de registro de control de entrada y salida del personal autorizado que haya tenido acceso al Data Center. En la bitácora debe registrarse el nombre, la firma, el motivo de ingreso, la hora de entrada y de salida.

9. Queda estrictamente prohibido el acceso al Data Center a los programadores o analistas, excepto bajo condiciones estrictamente de control.

10. Las listas de personal autorizado para ingresar al Data Center debe revisarse y depurarse trimestralmente, a efecto de evitar el acceso al personal que ya no esté autorizado, ya sea porque se ha retirado de la Institución o haya sido trasladado a otro puesto de trabajo.

11. Deben ubicarse cámaras de vigilancia permanente, alarmas o monitores que prevengan el acceso no autorizado.

12. Deben elaborarse carnet de visitantes para personas que visiten temporalmente el Data Center y deben ser acompañados por un miembro del personal autorizado, debe tenerse el cuidado de recuperar todos los carnets entregados a los visitantes; además no debe permitirse las visitas en grupos difíciles de controlar.

13. Las llaves o dispositivos de acceso al Data Center y a la Oficina de la Gerencia de Informática deben de permanecer en un lugar seguro y bajo la custodia del personal encargado.

14. Deben mantenerse medidas estrictas de seguridad dentro del Data Center, verificando que no exista material combustible, que los cableados eléctricos se encuentren protegidos con material aislante y bajo el piso falso, que el piso falso se encuentre limpio, que se encuentre a la mano un sistema contra incendio o que al menos haya extinguidores (vigentes), que esté alejado de baños, cañerías de agua y cocinas; y que exista señalización de evacuación por cualquier emergencia.

15. El personal encargado del Data Center debe recibir entrenamiento adecuado sobre los procedimientos que debe seguir en caso de incendio, inundación o cualquier incidente que cause alarma; debe conocer la ubicación de las alarmas contra incendio, extinguidores, interruptores reguladores y auxiliares de electricidad, de aire acondicionado, mascarillas, etc.

16. Deben existir contratos de mantenimiento preventivo y correctivo con los proveedores y el control debe llevarse en una bitácora de mantenimiento.

17. Los manuales de funcionamiento de los equipos del Data Center deben estar protegidos y solo pueden ser accesados por personal autorizado.

18. Dentro del Data Center debe existir suficiente espacio físico que sea acorde a la cantidad y tamaño de los equipos.

19. La seguridad de la bitácora debe estar protegida y periódicamente debe revisarse por la Jefatura de la Gerencia de Informática.

20. Cualquier duda de interpretación de la presente política debe ser resuelta por El Encargado de la Seguridad de Informática.

21. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 12

POLÍTICA PARA LA REALIZACIÓN DE PAGOS ELECTRONICOS.

Propósito

Establecer los parámetros de seguridad necesarios para la aplicación de Pagos Electrónicos a proveedores, realizados en los sitios web de las Instituciones autorizadas por la Superintendencia del Sistema Financiero, con las que se tengan contrato de servicios de esta forma de pago.

Alcance

Aplica para todos los Funcionarios y Servidores Públicos encargados de cargar los archivos de data y de realizar las autorizaciones correspondientes en el sitio web del sistema bancario.

Lineamientos

1. La función de los pagos electrónicos debe estar centralizada en la Gerencia Financiera y el de los refrendarios u autorizados.
2. Los servicios de pagos electrónicos deben estar debidamente respaldados por los contratos de servicios correspondientes, verificando que esté incluido la cláusula de confidencialidad de la información.
3. Se deben contratar pólizas de seguro de fidelidad por apropiación de recursos por parte de los servidores públicos y terceros.
4. Todos los pagos realizador por la vía electrónica deben estar PREVIAMENTE autorizados por escrito por los proveedores.
5. El número de cuenta bancaria de los proveedores en el maestro debe encontrase resguardada, limitando su visualización.
6. Antes de dar de alta a un proveedor en el maestro de proveedores, se deben verificar las listas restrictivas a las cuales se tenga el acceso.

7. Todos los pagos que se hagan por la vía de pagos electrónicos deben estar respaldados por la documentación soporte autorizada por la Gerencia Financiera.
8. Los cambios que se hagan a los maestros de proveedores, tales como creación, modificación o bloqueo, deben ser modificados y aprobados por un nivel independiente al que realiza los cambios.
9. Se deben asignar equipo específicos para la realización de pagos electrónicos.
10. Las instalaciones físicas donde se ubican los equipos para realizar los pagos, deben tener acceso restringido, cámaras de seguridad y bloqueos automáticos, entre otros.
11. El acceso a los equipos y/o portales para realizar los pagos, deben requerir al menos doble autenticación por parte de los usuarios autorizados.
12. Se deben establecer niveles de aprobación para la ejecución de operaciones electrónicas, de acuerdo con el monto.
13. Los pagos que se realizan deben tener un nivel de supervisión externo y periódico, independiente a quien los aprueba.
14. Se debe realizar autocontrol sobre las autorizaciones y documentación de soporte de los pagos realizados, considerando la verificación hacia los proveedores con mayores volúmenes de pago.
15. Todos los pagos deben ser autenticados para continuar con su proceso de aplicación.
16. No se deben manejar archivos planos.
17. Deben realizarse pruebas de seguridad a los lugares establecidos para el almacenamiento de la información, con el objeto de reducir la probabilidad de ataques, pérdida de información y accesos no autorizados.
18. Los filtros de spam deben tenerse activados.
19. El antivirus debe actualizarse automáticamente, verificando su efectividad en las aplicaciones de mayor vulnerabilidad.

20. Los niveles de seguridad del navegador con el cual se trabaja, deben ser verificadas periódicamente.
21. Los equipos donde se realizan los pagos deben ser parametrizados para tener acceso a una única red.
22. Deben verificarse los niveles de seguridad para las cuentas de correo electrónico en las cuales se transmite la información de los pagos.
23. Las claves de acceso deben tener las siguientes características:
    - Combinaciones de letras y números,
    - Son compuestas por mínimo 6 caracteres.
    - Restablecimiento de contraseñas al menos cada mes.
    - No se habilitan los accesos automáticos a los portales bancarios (usuarios y contraseña).
24. Deben generarse notificaciones automáticas a las cuentas de correo electrónico de los usuarios que realizan las aprobaciones de los pagos, cada vez que se ejecuta el pago o se generan cambios en el registro de las cuentas.
25. Deben conciliarse los registros contables con los registros bancarios cada vez que se realiza un pago por la vía electrónica.
26. Deben realizarse monitoreo periódicos sobre el ingreso al sistema, que permita identificar intentos fallidos de acceso, sesiones en fechas que no corresponden, entre otros, procediendo a realizar las investigaciones pertinentes.
27. Cada vez que un colaborador se retire de la Institución su usuario y registro para pagos debe ser bloqueado de inmediato.
28. Periódicamente debe verificarse con el Departamento de Recursos Humanos que todos los colaboradores desvinculados se hayan bloqueado para pagos electrónicos y aplicativos en general.

29. Deben utilizarse los controles de seguridad ofrecidos en el portal bancario, tales como restricción de horarios para operaciones, ip fija, confirmaciones y demás controles establecidos por la entidad bancaria.

30. Deben actualizarse los controles en el portal bancario y los aplicativos con las nuevas tendencias en seguridad y las recomendaciones de la entidad bancaria, actualizando en el último caso los contratos de prestación de servicios.

31. Queda determinantemente prohibida, la apertura de correos electrónicos desconocidos o de entidades bancarias que soliciten información de las cuentas bancarias de la organización.

32. Deben realizarse confirmaciones telefónicas con las entidades bancarias, cuando se cuestiona la veracidad de las comunicaciones electrónicas.

33. Cualquier duda de interpretación de la presente política debe ser resuelta por El Encargado de la Seguridad de la Información.

34. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

SECCIÓN 13

POLÍTICA PARA LA ASIGNACION Y RETIRO DE CUENTAS DE CORREO INSTITUCIONAL

Propósito

Establecer las directrices bajo las cuales se orienta la creación, administración y eliminación de cuentas de correo.

Alcance

Aplica para Oficina Central y los Centros de Atención a los Usuarios de Santa Ana y San Salvador, así como para todos los sistemas de información que soportan la operación. Su implementación será inmediata y obligatoria a partir de la fecha de publicación de la misma, razón por la cual los procedimientos existentes deberán ser revisados y ajustados a los lineamientos dados.

Lineamientos

1. Todo empleado o funcionario vinculado a SIGET, se le deberá asignar una cuenta de correo electrónico único que le permita la comunicación con internos y externos cuando se requiera para el desarrollo de sus funciones.

2. La autorización para la creación de su cuenta, será por medio un requerimiento formal de los Gerentes o Jefes de Área. Para todos los empleados o funcionarios que son vinculados por primera vez a SIGET así como la creación de listas de distribución de correo.

3. Se entiende por cuenta de correo electrónico la asignación por parte de SIGET:

   a. Una dirección electrónica con la forma usuario@siget.gob.sv
   b. Un buzón (espacio en disco) con capacidad máxima de almacenamiento de 10 MB
   c. Una palabra clave o password para acceder de manera privada a la cuenta.
   d. La posibilidad de enviar y recibir mensajes dentro de SIGET y hacia internet utilizando la dirección electrónica asignada.

4. La creación de la cuenta de correo electrónico es realizada por el Departamento de Redes y Soporte de la Gerencia de Informática, según el requerimiento realizado.

5. La cuenta de correo se construirá con las iniciales del nombre del usuario y el primer apellido sin tildes ni signos propios de ningún idioma, en caso de presentarse coincidencias en la identificación de dos usuarios se resolverá de acuerdo al orden de procesamiento: el primer usuarios recibirá la identificación antes mencionada, el segundo será alterado recurriendo a las primeras letras del segundo nombre. Por ejemplo:

   i. Jose Pablo Martinez (1er usuario) será jmartinez@siget.gob.sv
   ii. Jose Juan Martinez (2do usuario) será jjmartinez@siget.gob.sv

6. La Gerencia de Informática creará y configurará una firma de correo electrónica según la información proporcionada para la creación de la cuenta de correo.

7. Las cuentas de correo electrónico son personales e intransferibles y no se puede compartir su cuenta ni revelar su clave.

8. El Gerente o Jefe de Área es responsable de informar el retiro de los empleados o funcionarios a la Gerencia de Informática, garantizando así la oportuna eliminación de cuentas el día siguiente que termine oficialmente la vinculación con SIGET o cuando el Gerente o Jefe de Área así lo solicite.

9. Las listas de distribución de correo (grupos de trabajo) que tengan asignada una cuenta deben nombrar un usuario autorizado para manejarla.

10. Es responsabilidad de los usuarios:

    a. Usar su cuenta de correo electrónico institucional con fines laborales.

    b. Utilizar su firma electrónica de correo.

    c. Comportarse siempre en un ámbito profesional por medio de correo.

    d. Verificar que los remitentes y los datos adjuntos de los correos que envía sean los correctos así como indicar el asunto de los correos.

    e. Reportar al Departamento de Red y Soporte a Usuarios cualquier tipo de irregularidad o abuso de los servicios de correo o sospecha de suplantación de identidad.

11. Los usuarios no deben utilizar su cuenta de correo:

a. Para fines comerciales ni ajenos a SIGET.

b. Suscripciones a listas de correo que genere mensajes cuyo contenido no tenga que ver con las funciones de SIGET.

c. Con el fin de realizar algún tipo de acoso, violaciones a los derechos de autor, violación de patentes, difamación, calumnia, fraude, con intención de intimidar, insultar o cualquier otra forma de actividad hostil.

d. Para envió de correo spam o cadenas de correo no solicitado.

e. Para leer correos ajenos, ni generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.

12. La opción para enviar correo a Todo el personal de SIGET solo estará habilitada para cuentas autorizadas por la Superintendencia mediante formulario de autorización y se ejecutará la configuración por el Departamento de Redes y Soporte de la Gerencia de Informática.

13. La configuración de correo electrónico en dispositivos institucionales solo se realizará para cuentas autorizadas por los Gerentes o Jefes de área mediante formulario de autorización y se ejecutará la configuración por el Departamento de Redes y Soporte de la Gerencia de Informática.

14. La configuración de correo electrónico en dispositivos personales solo se realizará para cuentas autorizadas por la Superintendencia mediante formulario de autorización y se ejecutará la configuración por el Departamento de Redes y Soporte de la Gerencia de Informática.

15. Cualquier duda de interpretación de la presente política debe ser resuelta por el Gerente de la Gerencia de Informática.

16. El incumplimiento de la presente política genera sanciones disciplinarias, las cuales serán ejecutadas de acuerdo con lo establecido en el Reglamento Interno de Trabajo de SIGET, Código de Ética Gubernamental y demás legislación aplicable.

CAPITULO III OBJETIVO, FUNCIONES Y RELACIONES DE TRABAJO

SECCION 00 GERENCIA DE INFORMATICA

OBJETIVOS GENERAL

Brindar soporte en el área de informática para la Superintendencia General de Electricidad y Telecomunicaciones, con el fin de contribuir al desarrollo tecnológico y por ende al mejoramiento de la calidad en los servicios que brinda la institución.

OBJETIVOS ESPECIFICOS

- Cumplir con los requerimientos de servicio hechos por las Gerencias, Unidades y/o Departamentos que conforman SIGET, de acuerdo a los objetivos estratégicos institucionales

- Desarrollar planes de contingencia para la operación de los sistemas Institucionales.

FUNCIONES

- Establecer los mecanismos adecuados de comunicación y coordinación con las diferentes dependencias de la Institución, relacionados con el desempeño de las funciones de la dependencia.
- Administrar eficientemente todos los recursos (equipos, programas y servicios) informáticos con los que cuenta la SIGET y darles el mantenimiento correspondiente.
- Administrar todos los sistemas informáticos con los que cuenta y contará la Superintendencia, vigilando la estandarización de los mismos.
- Administrar eficientemente y velar por la integridad de la información contenida en las bases de datos de la SIGET.

Unidad de Planificación	Coordinación para la formulación de los Planes Operativos y Estratégicos.
Gerencia Administrativa	Seguir las indicaciones de dicha gerencia, en relación al control del activo fijo de su dependencia Solicitar los bienes o servicios necesarios para su funcionamiento. Coordinar procesos de capacitación de personal de la Unidad.
Gerencia Financiera	Coordinación de la formulación y ejecución del presupuesto.
Departamento de Comunicaciones y Relaciones Públicas	Apoyo en publicaciones internas y externas; apoyo en la organización de eventos, cuando éstos requieran uso de tecnología de información y comunicación, ya sea mediante el uso de recursos propios o subcontratados.
Unidad de Auditoria Interna	Revisiones de auditoría.
Unidad de Acceso a la Información y Transparencia	Poner a disposición información conforme a la Ley de Transparencia.

Relaciones Externas	
CON	**PARA**
Proveedores de toda clase de licencias, equipos, servicios de conexión a Internet, mantenimiento preventivo y correctivo de equipo de cómputo y capacitación	Adquisición, garantía y administración de procesos de compras de servicios
Entidades Gubernamentales	Coordinación de comunicación de sistemas informáticos.
Corte de Cuentas de la República	Colaborar y cumplir con los requerimientos de los procesos de control interno de acuerdo a las Normas Técnicas de Control Interno Especificas de la SIGET y requerimientos de la ley.

- Implementar proyectos de tecnología que permitan agilizar, optimizar y mejorar la calidad de los procesos clave en la institución, ya sea que se trate de desarrollo de sistemas a la medida, adecuación de sistemas ya existentes o implantación de soluciones comerciales. Todos los proyectos y sistemas quedarán debidamente documentados.
- Diseñar, junto con el personal de la Gerencia, los términos de referencia para la compra de equipo, software y servicios relacionados con Tecnologías de Información y Comunicación
- Investigar sobre nuevas tecnologías informáticas y evaluar su aplicación en SIGET, apoyados en capacitaciones constantes que se solicitarán para el personal del área de informática.
- Proporcionar soporte a todas y cada una de las áreas que conforman la SIGET.
- Desarrollar normativas para el diseño, administración de bases de datos, mantenimiento de software y hardware y reemplazo de equipo Informático.
- Supervisar, actualizar y evaluar el diseño de la página web de la SIGET.

RELACIONES DE TRABAJO:

Relaciones Internas	
CON	**PARA**
Superintendencia General	Recibir lineamientos y prioridades en el trabajo; presentación de informes.
Unidad de Adquisiciones y Contrataciones Institucional	Coordinar procesos de adquisiciones de bienes y servicios relacionadas con tecnologías de información y comunicación.
Todas las Unidades de Organización	Facilitar la puesta en marcha de soluciones tecnológicas, de acuerdo a prioridades establecidas Apoyo de sistemas informáticos y coordinación de publicaciones en la página WEB

SECCION 01 DEPARTAMENTO DE PROYECTOS TECNOLÓGICOS.

OBJETIVOS GENERAL

Realizar proyectos tecnológicos especiales de diferente naturaleza para todas las áreas de la institución y apoyar en el área técnica los proyectos especiales de otras Gerencias y Unidades.

OBJETIVOS ESPECIFICOS

Realizar la estimación del esfuerzo necesario para llevar a cabo los proyectos tecnológicos.

Seleccionar las estrategias de desarrollo de los proyectos, estructura y planes de trabajo con sus aproximaciones de tiempos.

FUNCIONES

- Área encargada de realizar el análisis, diseño e implementación de los proyectos, eventos, reuniones y otros similares.
- Responsables de coordinar todo lo referente a transmisiones en vivo, capacitaciones de diversa naturaleza y videoconferencias.
- Implementar proyectos de tecnología que permitan agilizar, optimizar y mejorar la calidad de los procesos clave en la institución.

RELACIONES DE TRABAJO

Relaciones Internas	
CON	**PARA**
Gerencia de Informática.	Recibir lineamientos. Gestionar aprobaciones.
Todas las Unidades y Gerencias de la Organización.	Respaldo de bases de datos institucionales, mantenimiento, inventario de equipos.
Relaciones Externas	
CON	**PARA**
Proveedores de bienes y servicios	Cotizaciones, Adquisiciones de bienes y servicios, garantías, coordinación de entrega de bienes y servicios.
Entidades Gubernamentales	Coordinación de comunicación de sistemas informáticos.
Casa presidencial	Lineamientos para el funcionamiento de las Unidades de Informática, Sistemas y Sitios institucionales
Corte de Cuentas de la República	Colaborar y cumplir con los requerimientos de los procesos de control interno de acuerdo a las Normas Técnicas de Control Interno Especificas de la SIGET y requerimientos de la ley.

SECCION 02 DEPARTAMENTO DE PROGRAMACIÓN Y DESARROLLO

OBJETIVOS GENERAL

Aplicar conocimientos, habilidades, técnicas y herramientas a las actividades de un proyecto, con el fin de planear, dirigir, organizar, satisfacer, cumplir y superar las necesidades de sistemas de información según las necesidades de SIGET.

OBJETIVOS ESPECIFICOS

- Apoyar la ejecución de proyectos de tecnología, de acuerdo a las necesidades y requerimientos informáticos establecidos por las Gerencias, Unidades y/o Departamentos que conforman SIGET.
- Formular los planes de trabajo de cada proyecto y los planes de prueba propios de cada proyecto o sistema en desarrollo, verificando su cumplimiento y la obtención de los resultados adecuados.

FUNCIONES

- Definir los proyectos a desarrollarse en las diferentes dependencias de la SIGET, de acuerdo al Plan de Trabajo.
- Administrar y supervisar los proyectos informáticos con los que cuenta y contará la Superintendencia, vigilando la estandarización de los mismos.
- Realizar todas las actividades de bases de datos, codificación y pruebas de los sistemas informáticos.
- Apoyar la implementación de los sistemas desarrollados.
- Apoyar o impartir las capacitaciones a usuarios de los sistemas nuevos o de sistemas actualizados.
- Elaborar manual de usuario y técnico de los sistemas elaborados en la SIGET.

RELACIONES DE TRABAJO

Relaciones Internas	
CON	**PARA**
Gerencia de Informática.	Recibir lineamientos. Gestionar aprobaciones.
Todas las Unidades y Gerencias de la Organización.	Respaldo de bases de datos institucionales, mantenimiento, inventario de equipos.
Relaciones Externas	
CON	**PARA**
Proveedores de bienes y servicios	Cotizaciones, Adquisiciones de bienes y servicios, garantías, coordinación de entrega de bienes y servicios.
Entidades Gubernamentales	Coordinación de comunicación de sistemas informáticos.
Casa presidencial	Lineamientos para el funcionamiento de las Unidades de Informática, Sistemas y Sitios institucionales
Corte de Cuentas de la República	Colaborar y cumplir con los requerimientos de los procesos de control interno de acuerdo a las NTCIE de la SIGET y requerimientos de la ley.

SECCION 03 DEPARTAMENTO DE ADMINISTRACIÓN DE RED Y SOPORTE A USUARIOS.

OBJETIVOS GENERAL

Asegurar que los usuarios de la red de datos institucional reciban el servicio con calidad y confiabilidad para respaldar las operaciones.

OBJETIVOS ESPECIFICOS

- Establecer las estrategias y tácticas de la ingeniería, operaciones, mantenimiento de la red y todos sus servicios así como de los equipos de red.
- Resolver posibles fallas de la red y asegurar que la información se mueva a través de ella con la máxima eficiencia y transparencia para los usuarios.
- Garantizar los respaldos de información institucionales, almacenados en los servidores institucionales.
- Proporcionar soporte y mantenimiento a los equipos informáticos, de forma que se minimice la posibilidad de fallas.
- Brindar soporte a los usuarios finales.
- Mantener en operación los sistemas informáticos, apoyados por sistemas alternos de contingencia.

FUNCIONES

- Administración de los equipos de la red de datos y servidores.
- Diseñar una estructura lógica para el almacenamiento de datos.
- Aplicar rutinas para el respaldo y resguardo de la información institucional.
- Implementar acciones para mejorar el performance de los servidores.
- Administrar las redes de datos y comunicaciones de SIGET.
- Apoyar al área de Desarrollo y Análisis de Sistemas durante la puesta en marcha de los mismos.
- Controlar el uso efectivo y buen funcionamiento de los equipos informáticos.

- Desarrollar y ejecutar planes de mantenimiento preventivo y correctivo del equipo informático.
- Brindar soporte técnico a los usuarios y equipos.
- Control de resguardo, préstamos y garantía de equipo informático.
- Establecer mecanismos de revisión para garantizar la utilización de software con licencias.

Relaciones Internas	
CON	**PARA**
Gerencia de Informática.	Recibir lineamientos. Gestionar aprobaciones.
Todas las Unidades de Organización.	Respaldo de bases de datos institucionales, mantenimiento, inventario de equipos.
Relaciones Externas	
CON	**PARA**
Proveedores de bienes y servicios	Cotizaciones, Adquisiciones de bienes y servicios, garantías, coordinación de entrega de bienes y servicios.
Entidades Gubernamentales	Coordinación de comunicación de sistemas informáticos.
Casa presidencial	Lineamientos para el funcionamiento de las Unidades de Informática, Sistemas y Sitios institucionales
Corte de Cuentas de la República	Colaborar y cumplir con los requerimientos de los procesos de control interno de acuerdo a las Normas Técnicas de Control Interno Especificas de la SIGET y requerimientos de la ley.

SECCION 04 DEPARTAMENTO EN SEGURIDAD INFORMÁTICA

OBJETIVOS GENERAL

Establecer el conjunto de medidas preventivas y reactivas que permiten resguardar y proteger la información de la Institución buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

OBJETIVOS ESPECIFICOS

- Aplicar barreras y procedimientos que resguarden el acceso a los datos y solo permita acceder a ellos a las personas autorizadas para hacerlo.
- Aplicar barreras físicas y procedimientos de control, como mediadas de prevención y contramedidas ante amenazas a los recursos e información de la institución.

FUNCIONES

- Establecer políticas de seguridad para la institución.
- Realizar tareas de auditorías permanentes y pruebas de penetración.
- Establecer planes de respuestas a incidentes
- Identificar, medir, controlar y gestionar los niveles de seguridad en materia informática o tecnologías de la información.

Relaciones Internas	
CON	**PARA**
Gerencia de Informática.	Recibir lineamientos. Gestionar aprobaciones.
Todas las Unidades y Gerencias de la Organización.	Respaldo de bases de datos institucionales, mantenimiento, inventario de equipos.
Relaciones Externas	
CON	**PARA**
Proveedores de bienes y servicios	Cotizaciones, Adquisiciones de bienes y servicios, garantías, coordinación de entrega de bienes y servicios.
Entidades Gubernamentales	Coordinación de comunicación de sistemas informáticos.
Casa presidencial	Lineamientos para el funcionamiento de las Unidades de Informática, Sistemas y Sitios institucionales
Corte de Cuentas de la República	Colaborar y cumplir con los requerimientos de los procesos de control interno de acuerdo a las Normas Técnicas de Control Interno Especificas de la SIGET y requerimientos de la ley.

CAPITULO IV BASE LEGAL

SECCION 00 SECCION UNICA

La base legal que sustenta a la Gerencia de Informática, descansa en los siguientes acuerdos y decretos:

- Ley de Creación de la Superintendencia General de Electricidad y Telecomunicaciones, emitidos por la Asamblea Legislativa, según Decreto 808 del 12 de septiembre de 1996, publicadas en el Diario Oficial No.189, tomo 333 del 9 de octubre de 1996.
- Reglamento de la Ley de Creación de la Superintendencia General de Electricidad y Telecomunicaciones, emitido por Decreto Ejecutivo 56 del 13 de mayo de 1998, publicadas en el Diario Oficial No.88, tomo 339 del 15 de mayo de 1998.
- Ley General de Electricidad, emitido por la Asamblea Legislativa, según Decreto 843 del 10 de octubre de 1996, publicadas en el Diario Oficial No.201, tomo 333 del 25 de octubre de 1996.
- Reglamento de la Ley General de Electricidad, emitido por Decreto Ejecutivo 70 del 25 de julio de 1997, publicadas en el Diario Oficial No.138, tomo 336 del 25 de julio de 1997.
- Ley de Telecomunicaciones, emitido por la Asamblea Legislativa, según Decreto 142 del 6 de noviembre de 1997, publicadas en el Diario Oficial No.218, tomo 337 del 21 de noviembre de 1997.
- Reglamento de la Ley de Telecomunicaciones, emitido por Decreto Ejecutivo 64 del 15 de mayo de 1998, publicadas en el Diario Oficial No.88, tomo 339 del 15 de mayo de 1998.
- Normas Técnicas de Control Interno Específicas de SIGET.

CAPITULO V DESCRIPCIÓN BÁSICA DE LOS PUESTOS DE TRABAJO

A continuación se presentan el perfil del puesto con el propósito de definir las tareas y responsabilidades de cada integrante y por ende, los requisitos que deben cumplir quienes sean responsables de su desempeño.

SECCION 00 GERENCIA DE INFORMÁTICA

01

GERENTE DE INFORMÁTICA

Título del Puesto

GERENCIA DE INFORMÁTICA

-17-

Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

GERENTE	**-1-**	**AGOSTO 2017**
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. ***Por qué*** *existe el puesto y* ***qué debe lograr****, recuerde que NO se requiere una lista de actividades, sino la* ***Misión principal del puesto****.*

Planificar, organizar, dirigir y controlar las diferentes actividades y cumplir con los objetivos y metas de la Gerencia así como la supervisión del personal a su cargo.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 30%

Supervisar y apoyar al personal, lo que incluye la asignación de actividades, medir los objetivos asignados a cada persona y el desempeño de sus actividades o deberes, mediante evaluaciones de desempeño y cumplimientos de objetivos logrados, sugerir capacitaciones orientadas al mejoramiento continuo de las capacidades del personal.

Tareas Permanentes:

- *Medir los objetivos asignados a los empleados*
- *Manejar el desempeño de la Gerencia*
- *Acompañar en el curso de las actividades y deberes de los empleados.*
- *Coordinar las evaluaciones de personal.*
- *Elaborar y proponer acciones de capacitación orientadas al mejoramiento continuo de las capacidades del personal de la Gerencia.*

Responsabilidad de Trabajo # 2 — 25%

Formular, dar seguimiento, y evaluar la ejecución del Plan Estratégico Institucional (PEI) y al Plan Operativo Anual (POA) de la Gerencia, e investigar nuevas tecnologías y programas que puedan ser desarrollados o implementados a beneficios de SIGET.

Tareas Permanentes:

- *Investigar nuevas tecnologías y programas que puedan ser desarrollados o implementados a beneficios de SIGET*
- *Formular el plan estratégico y operativo.*
- *Dar seguimiento al plan estratégico.*
- *Dar seguimiento al plan operativo y los informes mensuales de avance de la matriz Plan Operativo Anual.*
- *Evaluar la ejecución del plan estratégico y del plan operativo.*

Responsabilidad de Trabajo # 3 — 15%

Formular y dar seguimiento al presupuesto de la Gerencia, definición de directrices para la contratación de servicios y adquisición de hardware y equipos.

Tareas Permanentes:

- *Formular el presupuesto de la Gerencia*
- *Dar seguimiento al presupuesto de la Gerencia*
- *Definir directrices para la contratación de servicios y adquisición de hardware y equipos.*
- *Enviar el listado de activos intangibles de la Gerencia por cada ejercicio fiscal.*

Responsabilidad de Trabajo # 4 — 15%

Gestionar la plataforma tecnológica para la mejora e innovación de procesos y servicios, solución a las necesidades informáticas de la Institución mediante la coordinación y planeación estratégica, coordinación, supervisión y evaluación de lineamientos y procesos

Tareas Permanentes:

- *Resolver las necesidades informáticas de la Institución mediante la coordinación y planeación estratégica.*
- *Supervisar y evaluar el alineamiento de los sistemas de información y los procesos.*
- *Propiciar la investigación, desarrollo y aplicación de nuevas tecnologías asociadas con la mejora de capacidades y generación de ventajas competitivas para la Institución.*
- *Establecer planes de contingencia para las funciones críticas.*
- *Mantener las medidas necesarias para la continuidad de la gestión Institucional, así como para los procesos y procedimientos de recuperación de desastres.*

Responsabilidad de Trabajo # 5 — 10%

Definir políticas y normas de seguridad de la Información: Establecer, dar seguimiento y coordinar todos los aspectos relacionados a políticas y normas de la seguridad de la información.

Tareas Permanentes:

- *Establecer procedimientos generales de seguridad física y lógica*
- *Dar seguimiento al cumplimiento de las políticas y normas de seguridad de la Información.*
- *Coordinar la realización de controles de seguridad.*

Responsabilidad de Trabajo # 6 — 5%

Atender solicitudes y requerimientos de las Gerencias y Unidades: para la obtención de equipos, servicios, programas, coordinación de apoyo técnico, capacitaciones y reuniones de diversa naturaleza entre otros.

Tareas Permanentes:

- *Colaborar con las dependencias de SIGET, para la obtención de nuevos equipos, servicios, programas, etc.*
- *Coordinar el apoyo técnico en eventos de capacitaciones de diversa naturaleza.*
- *Coordinar el apoyo técnico en Reuniones de diversa naturaleza así como transmisiones en vivo.*
- *Asesorar y recomendar a la Alta Dirección en las soluciones tecnológicas, propiciando la innovación de procesos y servicios.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 3 de resolución de Problema: Porqué las cosas que se hacen son conocidas, pero lo que se debe hacer y cómo debe hacerse no está definido. La persona debe ser analítico, crítico, investigativo y generador ideas, recomendaciones o soluciones a los problemas identificados.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☒ PRINCIPAL (asume completa y total responsabilidad)

☐ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación **Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"**

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Maestría o Post-grado en Administración de Empresas o Sistemas Informáticos, o áreas afines.
Educación Superior	☒	☐	Profesional Graduado en Ingeniería o , Licenciado en Sistemas Informáticos, o equivalente de educación

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia mínima de 5 años como Gerente o Jefe de Informática o puestos similares.

Deseable:

- Experiencia en la administración de redes informáticas que incluyan servicios de correo electrónico y web, sistemas de información que funcionen con administradores de bases de datos relacionales y seguridad para ambiente internet, diseño y desarrollo de sistemas informáticos.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Idioma Ingles a nivel Intermedio.
- Experiencia en Administración de Proyectos y Planificación
- Elaboración de Presupuestos.
- Diseño y desarrollo de sistemas informáticos
- Administración de Redes Informáticas

Deseable:

- Conocimiento y experiencia en la aplicación de leyes, reglamentos e instructivos relacionados con la naturaleza del puesto.

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

GERENCIAS, JEFES UNIDADES ASESORAS, JEFES DEPTO *(este grupo de comportamientos incluye al personal que desempeñan puestos con carácter de Gerencia y Jefaturas de Unidades Asesoras o Departamentos).*

APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.

Comportamientos evaluados:

1. Conoce las funciones de su puesto?
2. Demuestra dominio de conocimientos técnicos y especializados?
3. Es hábil para buscar alternativas de solución?
4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
5. En momentos de crisis los problemas los resuelve con habilidad?

CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.

6. Es experto en los conocimientos concernientes a su área de trabajo, y permanentemente se actualiza en estos y en otros temas de interés que contribuyan a alcanzar los objetivos institucionales?
7. Aplica los conceptos teóricos modernos y las mejores prácticas al desarrollo de sus actividades?
8. Realiza propuestas de mejoramiento y está abierto a valorar las propuestas de otros para optimizar el desempeño?
9. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios?
10. Posee capacidad para resolver situaciones a corto y largo plazo?

ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incremento de eficiencia en el personal.

A

11. Es puntual en sus compromisos de trabajo?
12. Organiza y programa adecuadamente su trabajo?
13. Mantiene una actitud receptiva hacia la información o puntos de vista de otras personas?
14. Inspira y transmite confianza en sus relaciones interpersonales?
15. Es respetuoso y considerado con sus colaboradores?

ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).

16. Planifica sus acciones y las de su equipo de trabajo , considerando las necesidades de sus clientes (internos y/o externos)?
17. Mantiene una comunicación efectiva con el cliente (interno y/o externo) para conocer sus necesidades y su nivel de satisfacción.
18. Logra que los clientes (internos y/o externos) sientan que son lo más importante para la institución, manteniendo excelentes
19. Actua como referente interno y/o externo cuando se busca aportar soluciones o satisfacer necesidades de sus clientes?
20. Trabaja con una perspectiva de largo plazo a la hora de resolver los problemas del cliente (interno y/o externo), considerando sus impactos?

LIDERAZGO : Entendido como la habilidad necesaria para orientar la acción de equipo de trabajo en una acción determinada, inspirando los valores en acción y anticipando escenarios de desarrollo de su equipo de trabajo.

21. Lidera adecuadamente las reuniones (define agenda, establece fechas, los objetivos a discutir, controla el tiempo y asigna turnos de palabra, etc.)?
22. Fija objetivos, los transmite claramente, realiza el seguimiento y brinda coaching sobre avances?
23. Escucha y promueve la participación y la aportación de ideas?
24. Delega y empodera a su equipo transmitiendo confianza y realizando un seguimiento efectivo?
25. Tiene carisma propio, comunica una visión de futuro que genera entusiasmo y compromiso con la misión de la institución?

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Unidad de Auditoria Interna**	Revisiones de auditoría.
	Todas las Unidades y Gerencias de la Organización	Coordinar y gestionar que se brinden los servicios de informática a todas las áreas. Mantener en operación los sistemas informáticos y apoyar la continuidad de la gestión Institucional en todas las áreas.
Externos	**Proveedores de servicios y bienes**	Adquirir productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.
	Entidades Gubernamentales	Coordinación de comunicación de sistemas informáticos y colaboración de proyectos
	Corte de Cuentas de la República	Colaborar y cumplir con los requerimientos de los procesos de control interno de acuerdo a las NTCIE de la SIGET y requerimiento de la ley.

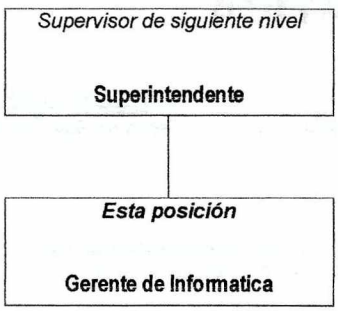
Condiciones de Trabajo

Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina **90%**

Porcentaje esperado de tiempo en viajes (al interior y exterior del país) **10%**

Organización Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCION 00

02

ANALISTA DE INFORMÁTICA

Título del Puesto

GERENCIA DE INFORMÁTICA

-13-

Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

EXPERTO	**-1-**	**AGOSTO 2017**
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. ***Por qué*** *existe el puesto y* ***qué debe lograr****, recuerde que NO se requiere una lista de actividades, sino la* ***Misión principal del puesto****.*

Mantener un control de requisiciones y licitaciones de equipo, licencias y/o servicios informáticos, así también poseer un control y registro de los gastos presupuestales del hardware, software y servicios informáticos contratados, participar eficientemente en el cumplimiento de los objetivos y metas de la Gerencia.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 35%

Elaborar en conjunto con el Gerente de Informática el Plan Estratégico Institucional y el Plan Operativo Anual: apoyar a la Gerencia en todas las tareas relacionadas al de Plan Operativo Anual (POA) y Plan Estratégico Institucional (PEI).

Tareas Permanentes:

- *Apoyar en la formulación del plan estratégico y operativo*
- *Consolidar el informe de avances del plan estratégico.*
- *Consolidar y elaborar el informe mensual de avances de la matriz Plan Operativo Anual*
- *Asistir a Reuniones relacionadas al seguimiento del Plan Operativo Anual*
- *Preparar la información para auditorias de Plan Operativo Anual y Plan Estratégico Institucional.*

Responsabilidad de Trabajo # 2 — 25%

Elaborar, apoyar, y consolidar en conjunto con Gerente de Informática el presupuesto de la Gerencia, asistir a reuniones relacionadas al presupuesto Institucional, y responsable de llevar el control de la disponibilidad del presupuesto; también solicitar las necesidades de hardware y software a los Jefes de la Gerencia de Informática.

Tareas Permanentes:

- *Apoyar en la formulación del presupuesto de la Gerencia de Informática*
- *Solicitar las necesidades de hardware y software a los Jefes de la Gerencia de Informática*
- *Consolidar el presupuesto*
- *Responsable de ingresar el mismo en los sistemas de presupuesto*
- *Asistir a Reuniones relacionadas al presupuesto institucional.*
- *Responsable de llevar control de disponibilidad de presupuesto*

Responsabilidad de Trabajo # 3 — 20%

Gestionar la adquisición y contratación de equipos y/o servicios para la Gerencia de Informática: y apoyar solicitudes de otras áreas de la Institución.

Tareas Permanentes:

- *Responsable de iniciar y dar seguimiento a los procesos de compras de la Gerencia o solicitud de cualquier área de la Institución*
- *Crear y en algunos casos acompañar la creación de términos de referencia para los procesos de compra.*
- *Asistir en evaluaciones de ofertas técnicas.*
- *Ser enlace entre la Gerencia de Informática, proveedores y la Unidad de Adquisiciones y Contrataciones Institucional.*

Responsabilidad de Trabajo # 4 — 20%

Recibir, archivar y distribuir la correspondencia general de la Gerencia, elaboración de correspondencia y memorandos, requerir y administrar los artículos de oficina.

Tareas Permanentes:

- *Recibir, archivar y distribuir la correspondencia general de la Gerencia*
- *Elaboración de correspondencia y memorandos.*
- *Administrar y ejecutar correctamente la marginación de la correspondencia de la Gerencia*
- *Requerir y administrar los artículos de oficina.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 2 de resolución de Problema: Porqué lo que hay que hacer es conocido, pero como hacerlo no está definido. La persona debe de usar habilidades de interpolación para escoger la estrategia correcta para tratar el problema dado.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☐ PRINCIPAL (asume completa y total responsabilidad)

☒ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Graduado en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.
Educación Superior	☒	☐	Cursando Tercer año en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia mínima de 3 años como Analista de Informática o en puestos similares;

Deseable:

- Experiencia a nivel de usuarios con el uso de tecnologías de internet, conocimiento en procesos de compra o ventas de productos y servicios informáticos, experiencia en soporte a usuarios finales.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Idioma ingles a nivel intermedio.
- Elaboración de presupuestos.
- Planeación Estratégica

Deseable:

- Conocimiento y experiencia en la aplicación de leyes, reglamentos e instructivos relacionados con la naturaleza del puesto.
- Conocimiento de la Ley de Adquisiciones y Contrataciones de la Administración Pública (LACAP) y su Reglamento.

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

PERSONAL TECNICO Y ADMINISTRATIVO *(este grupo incluye al personal que desarrollan labores técnicas y/o Administrativas en áreas especializadas de la institución).*

APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.

Comportamientos evaluados:

1. Conoce las funciones de su puesto?
2. Demuestra dominio de conocimientos técnicos y especializados?
3. Posee capacidad propósitiva y criterio propio para solucionar las dificultades con sensatez y acudir en forma independiente y eficaz, sin necesidad de que se le proporcionen instrucciones?
4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
5. Proporciona respuestas oportunas a las exigencias de trabajo?

CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.

6. Identifica las tareas esenciales a realizar en el trabajo?
7. Se dedica a cumplir con su trabajo en el plazo establecido, evitando distraerse con asuntos personales?
8. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios al finalizarla?
9. Comprende la interrelación existente de trabajo entre su área y otras areas de la institución?.
10. Frecuentemente realiza un esfuerzo mas allá de lo normal, para dar por finalizada una tarea asignada o problemas especificos?

ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incrmento de eficiencia en el personal.

11. Es puntual en sus compromisos de trabajo?
12. Organiza y programa adecuadamente su trabajo?
13. Sabe como trabajar formando parte de un equipo?
14. Inspira y transmite confianza en sus relaciones interpersonales?
15. Es respetuoso y considerado con sus superiores y compañeros de trabajo?

ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).

16. Entiende con facilidad los problemas y/o necesidades de sus clientes (internos y/o externos)?
17. Desarrolla soluciones a los problemas de los clientes (internos y/o externos), trabajando junto con ellos?
18. Asesora y da al cliente (interno y/o externo) las alternativas que mejor se adaptan a sus necesidades?
19. Se apega a los tiempos estipulados para la entrega de los servicios solicitados por los clientes (internos y/o externos), exigiéndose cumplir en tiempo y calidad?
20. Hace más de lo que normalmente el cliente (nterno y/o externo) espera?

B

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes**	Adquirir productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

Condiciones de Trabajo

Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina	**98%**
Porcentaje esperado de tiempo en viajes (al interior y exterior del país)	**2%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.

SECCION 01 DEPARTAMENTO DE PROYECTOS TECNOLÓGICOS

01

JEFE DE DEPARTAMENTO DE PROYECTOS TECNOLÓGICOS

Título del Puesto

GERENCIA DE INFORMÁTICA

-16-

Gerencia /Unidad Asesora/Jefatura Técnica

Grado/Nivel Puesto

JEFE	**-1-**	**AGOSTO 2017**
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

*En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. **Por qué** existe el puesto y **qué debe lograr**, recuerde que NO se requiere una lista de actividades, sino la **Misión principal del puesto**.*

Realizar la estimación del esfuerzo necesario para llevar a cabo los proyectos, seleccionar las estrategias de desarrollo, determinar la estructura de los mismos, fijando el calendario y estableciendo la planificación del proyecto.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.
Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 30%

Supervisar y asignar actividades al personal a su cargo, medir los objetivos asignados a cada persona y el desempeño de sus actividades o deberes, mediante evaluaciones de desempeño y cumplimientos de objetivos logrados, sugerir capacitaciones orientadas al mejoramiento continuo de las capacidades del personal.

Tareas Permanentes:

- *Encargado de asignar actividades a los empleados a su cargo.*
- *Medir los objetivos asignados a los empleados a su cargo.*
- *Manejo del desempeño.*
- *Acompañamiento en el curso de las actividades y deberes de los empleados.*
- *Coordinar las evaluaciones de personal a su cargo.*
- *Encargado de sugerir acciones de capacitación orientadas al mejoramiento continuo de las capacidades del personal a su cargo*

Responsabilidad de Trabajo # 2 — 25%

Realizar proyectos: encargado del análisis, diseño e implementación de proyectos especiales, eventos reuniones y transmisiones nacionales o internacionales.

Tareas Permanentes:

- *Colaborar con las partes involucradas para la definición y concertación de los objetivos del proyecto.*
- *Planificar proyectos en todos sus aspectos, identificando las actividades a realizar, los recursos, los plazos y costes previstos.*
- *Dirección y coordinación de todos los recursos empleados en el proyecto.*
- *Mantenimiento permanente de las relaciones externas del proyecto como proveedores, subcontratistas y otros involucrados.*
- *Seguimiento de las acciones.*
- *Adoptar medidas correctoras pertinentes para el cumplimiento del proyecto.*
- *Responder ante superiores de la consecución de los objetivos del proyecto.*
- *Evaluar la gestión de riesgos del proyecto.*
- *Documentar la gestión del proyecto una vez que se ha finalizado.*

Responsabilidad de Trabajo # 3 — 25%

Ejecutar y dar seguimiento a las acciones asignadas del plan Estratégico Institucional y al Plan Operativo Anual de la Gerencia: realizar todas las acciones necesarias para su cumplimiento.

Tareas Permanentes:

- *Dar seguimiento a las actividades asignadas del Plan Estratégico.*
- *Dar seguimiento a las actividades asignadas del Plan Operativo.*
- *Elaborar informe de la ejecución del Plan Estratégico y del Plan Operativo.*

Responsabilidad de Trabajo # 4 — 20%

Coordinar las transmisiones en vivo, capacitaciones de diversa naturaleza y videoconferencias: tanto de eventos nacionales como internacionales.

Tareas Permanentes:

- *Colaborar con las dependencias de SIGET, en relación a las solicitudes de transmisión en vivo o videoconferencias*
- *Coordinar el apoyo técnico necesario.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 3 de resolución de Problema: Porqué las cosas que se hacen son conocidas, pero lo que se debe hacer y cómo debe hacerse no está definido. La persona debe ser analítico, crítico, investigativo y generador ideas, recomendaciones o soluciones a los problemas identificados.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☒ PRINCIPAL (asume completa y total responsabilidad)

☐ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Maestría o Post-grado en Administración de Empresas o Sistemas Informáticos, o áreas afines.
Educación Superior	☒	☐	Profesional Graduado en Ingeniería o, Licenciado en Sistemas Informáticos, o equivalente de educación.

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia mínima de 5 años como Jefe de Proyectos Tecnológicos o en puestos similares.

Deseable:

- Experiencia con sistemas operativos.
- Experiencia con instalación, configuración de software y hardware.
- Dominio en el manejo de herramientas para la administración de proyectos.
- Experiencia en desarrollo de sistemas, definición y formulación de proyectos.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Idioma Ingles a nivel Intermedio.
- Conocimiento en proyectos de transformación digital.

Deseable:

- Conocimiento y experiencia en la aplicación de leyes, reglamentos e instructivos relacionados con la naturaleza del puesto.
- Experiencia con equipos de videoconferencia y transmisiones en vivo en línea.

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

A

GERENCIAS, JEFES UNIDADES ASESORAS, JEFES DEPTO ***(este grupo de comportamientos incluye al personal que desempeñan puestos con carácter de Gerencia y Jefaturas de Unidades Asesoras o Departamentos).***

APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.

Comportamientos evaluados:

1. Conoce las funciones de su puesto?
2. Demuestra dominio de conocimientos técnicos y especializados?
3. Es hábil para buscar alternativas de solución?
4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
5. En momentos de crisis los problemas los resuelve con habilidad?

CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.

6. Es experto en los conocimientos concernientes a su área de trabajo, y permanentemente se actualiza en estos y en otros temas de interés que contribuyan a alcanzar los objetivos institucionales?
7. Aplica los conceptos teóricos modernos y las mejores prácticas al desarrollo de sus actividades?
8. Realiza propuestas de mejoramiento y está abierto a valorar las propuestas de otros para optimizar el desempeño?
9. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios?
10. Posee capacidad para resolver situaciones a corto y largo plazo?

ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incrmento de eficiencia en el personal.

11. Es puntual en sus compromisos de trabajo?
12. Organiza y programa adecuadamente su trabajo?
13. Mantiene una actitud receptiva hacia la información o puntos de vista de otras personas?
14. Inspira y transmite confianza en sus relaciones interpersonales?
15. Es respetuoso y considerado con sus colaboradores?

ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).

16. Planifica sus acciones y las de su equipo de trabajo , considerando las necesidades de sus clientes (internos y/o externos)?
17. Mantiene una comunicación efectiva con el cliente (interno y/o externo) para conocer sus necesidades y su nivel de satisfacción.
18. Logra que los clientes (internos y/o externos) sientan que son lo más importante para la institución, manteniendo excelentes
19. Actua como referente interno y/o externo cuando se busca aportar soluciones o satisfacer necesidades de sus clientes?
20. Trabaja con una perspectiva de largo plazo a la hora de resolver los problemas del cliente (interno y/o externo), considerando sus impactos?

LIDERAZGO : Entendido como la habilidad necesaria para orientar la acción de equipo de trabajo en una acción determinada, inspirando los valores en acción y anticipando escenarios de desarrollo de su equipo de trabajo.

21. Lidera adecuadamente las reuniones (define agenda, establece fechas, los objetivos a discutir, controla el tiempo y asigna turnos de palabra, etc.)?
22. Fija objetivos, los transmite claramente, realiza el seguimiento y brinda coaching sobre avances?
23. Escucha y promueve la participación y la aportación de ideas?
24. Delega y empodera a su equipo transmitiendo confianza y realizando un seguimiento efectivo?
25. Tiene carisma propio, comunica una visión de futuro que genera entusiasmo y compromiso con la misión de la institución?

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización.**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes**	Adquirir productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

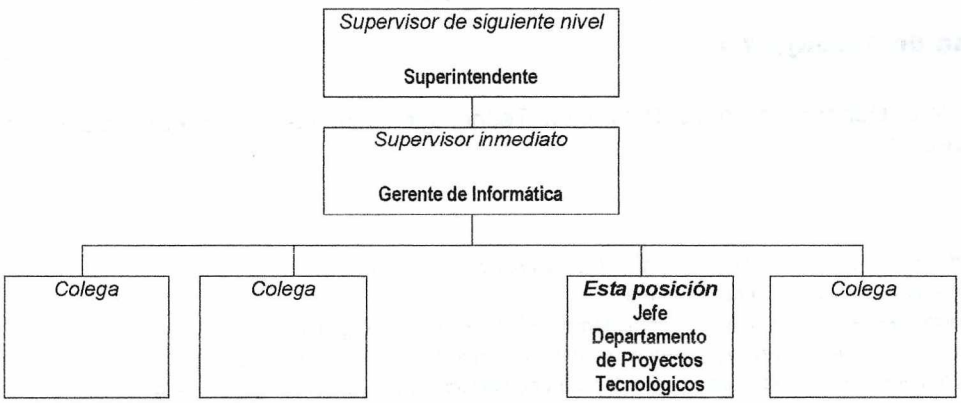
Condiciones de Trabajo

Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina	**90%**
Porcentaje esperado de tiempo en viajes (al interior y exterior del país)	**10%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 01

02

TÉCNICO DE PROYECTOS TECNOLÓGICOS

Título del Puesto

GERENCIA DE INFORMÁTICA

-11-
Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

EXPERTO	-1-	AGOSTO 2017
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

*En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. **Por qué** existe el puesto y **qué debe lograr**, recuerde que NO se requiere una lista de actividades, sino la **Misión principal del puesto.***

Responsable de realizar tareas para la realización de proyectos tecnológicos especiales, colaborar directamente con el Jefe de Departamento en proyectos y de ejecutar calendarios y actividades de proyectos.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.
Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 40%

Colaborar con el Jefe Departamento de Proyectos Tecnológicos en las actividades relacionadas a la realización de proyectos.

Tareas Permanentes:

- *Brindar soporte con las partes involucradas para el cumplimiento de los objetivos del proyecto.*
- *Realizar las tareas asignadas en tiempo y forma.*
- *Reportar las acciones realizadas al Jefe Departamento de Proyectos Tecnológicos*
- *Implementación de medidas correctoras pertinentes para el cumplimiento del proyecto de existir.*
- *Responder ante superiores de las tareas asignadas para consecución de los objetivos del proyecto.*
- *Encargado de entregar toda la información necesaria para documentar la gestión del proyecto una vez que se ha finalizado.*

Responsabilidad de Trabajo # 2 — 35%

Colaborar en las transmisiones en vivo y videoconferencias: nacionales e internacionales.

Tareas Permanentes:

- *Brindar soporte en las dependencias de SIGET, en relación a las solicitudes de transmisión en vivo o videoconferencias.*
- *Encargado de recomendar apoyo técnico adicional a su superior para divulgación de transmisiones en vivo en página web y otros.*
- *Coordinar y controlar empresas contratadas para la realización de transmisiones en vivo y videoconferencias.*
- *Encargo de pruebas de equipos de comunicación.*
- *Reportar a su superior las actividades realizadas.*

Responsabilidad de Trabajo # 3 — 25%

Colaborar en eventos de capacitación cuando se requiera.

Tareas Permanentes:

- *Apoyar a otras unidades o gerencias de la institución en eventos que requieran uso de equipo informático.*
- *Asistir con equipos de proyección.*
- *Apoyo para revisión de instalaciones donde se vayan a realizar eventos de capacitación o similares.*
- *Reportar a su superior las actividades realizadas.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

La plaza se encuentra en un nivel 2 de resolución de Problema: Porqué lo que hay que hacer es conocido, pero como hacerlo no está definido. La persona debe de usar habilidades de interpolación para escoger la estrategia correcta para tratar el problema dado.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☐ PRINCIPAL (asume completa y total responsabilidad)

☒ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Graduado en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.
Educación Superior	☒	☐	Cursando Tercer año en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia mínima de 3 años como Técnico de Proyectos o en puestos similares.

Deseable:

- Experiencia a nivel de usuarios con el uso de tecnologías de internet,
- Conocimiento en procesos de compra o ventas de productos y servicios informáticos.
- Experiencia en soporte a usuarios finales.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Idioma ingles a nivel intermedio
- Elaboración de presupuestos.

Deseable:

- Conocimiento y experiencia en la aplicación de leyes, reglamentos e instructivos relacionados con la naturaleza del puesto.
- Experiencia con equipos de videoconferencia y transmisiones en vivo en línea.

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

PERSONAL TECNICO Y ADMINISTRATIVO *(este grupo incluye al personal que desarrollan labores técnicas y/o Administrativas en áreas especializadas de la institución).*

B

APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten pone práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.

Comportamientos evaluados:

1. Conoce las funciones de su puesto?
2. Demuestra dominio de conocimientos técnicos y especializados?
3. Posee capacidad propósitiva y criterio propio para solucionar las dificultades con sensatez y acudir en forma independient eficaz, sin necesidad de que se le proporcionen instrucciones?
4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
5. Proporciona respuestas oportunas a las exigencias de trabajo?

CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.

6. Identifica las tareas esenciales a realizar en el trabajo?
7. Se dedica a cumplir con su trabajo en el plazo establecido, evitando distraerse con asuntos personales?
8. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios al finalizarla?
9. Comprende la interrelación existente de trabajo entre su área y otras areas de la institución?.
10. Frecuentemente realiza un esfuerzo mas allá de lo normal, para dar por finalizada una tarea asignada o problemas espe

ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valo el quehacer laboral y contribuir al incrmento de eficiencia en el personal.

11. Es puntual en sus compromisos de trabajo?
12. Organiza y programa adecuadamente su trabajo?
13. Sabe como trabajar formando parte de un equipo?
14. Inspira y transmite confianza en sus relaciones interpersonales?
15. Es respetuoso y considerado con sus superiores y compañeros de trabajo?

ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entre los servicios a nuestros clientes internos (areas internas de la SIGET).

16. Entiende con facilidad los problemas y/o necesidades de sus clientes (internos y/o externos)?
17. Desarrolla soluciones a los problemas de los clientes (internos y/o externos), trabajando junto con ellos?
18. Asesora y da al cliente (interno y/o externo) las alternativas que mejor se adaptan a sus necesidades?
19. Se apega a los tiempos estipulados para la entrega de los servicios solicitados por los clientes (internos y/o externos), exigiéndose cumplir en tiempo y calidad?
20. Hace más de lo que normalmente el cliente (nterno y/o externo) espera?

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización.**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes.**	Adquisiciones de productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

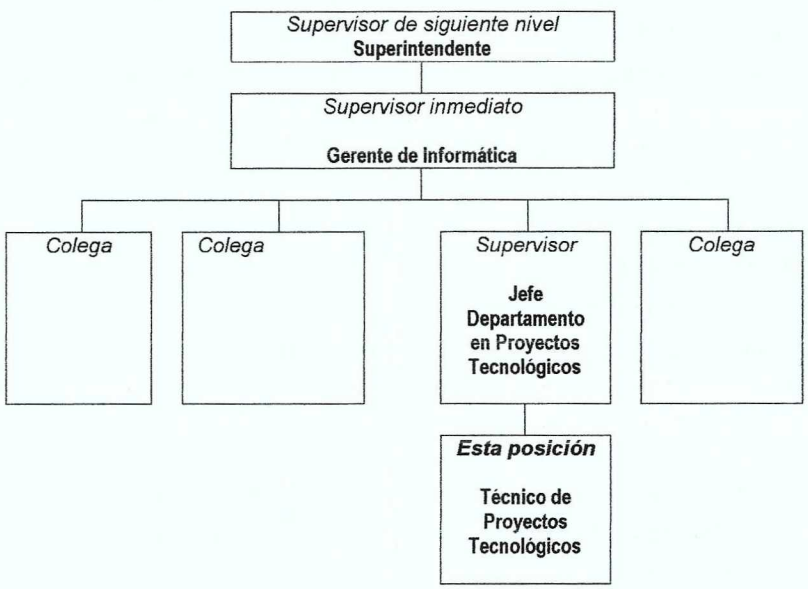
Condiciones de Trabajo

Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina	**98%**
Porcentaje esperado de tiempo en viajes (al interior y exterior del país)	**2%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 02 DEPARTAMENTO DE PROGRAMACIÓN Y DESARROLLO

01

JEFE DEPARTAMENTO DE PROGRAMACIÓN Y DESARROLLO

Título del Puesto

GERENCIA DE INFORMÁTICA

-16-

Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

JEFE	-1-	AGOSTO 2017
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

*En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. **Por qué** existe el puesto y **qué debe lograr**, recuerde que NO se requiere una lista de actividades, sino la **Misión principal del puesto**.*

Diseñar y administrar el desarrollo de sistemas informáticos, participar eficientemente en el cumplimiento de los objetivos y metas de la Gerencia.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 30%

Supervisar y asignar actividades al personal a su cargo, medir los objetivos asignados a cada persona y el desempeño de sus actividades o deberes, mediante evaluaciones de desempeño y cumplimientos de objetivos logrados, sugerir capacitaciones orientadas al mejoramiento continuo de las capacidades del personal.

Tareas Permanentes:

- *Asignar actividades a los empleados a su cargo.*
- *Medir los objetivos asignados a los empleados a su cargo.*
- *Manejar el desempeño del personal a su cargo.*
- *Acompañar las actividades y deberes de los empleados.*
- *Coordinar las evaluaciones de personal a su cargo.*
- *Sugerir acciones de capacitación orientadas al mejoramiento continuo de las capacidades del personal a su cargo.*

Responsabilidad de Trabajo # 2 — 25%

Coordinar, supervisar y controlar el desarrollo de proyectos informáticos de acuerdo a las necesidades de la institución, atender y dar respuesta a los requerimientos de la Gerencia y de las distintas dependencias de SIGET.

Tareas Permanentes:

- *Desarrollo de informes de control de avances de los diferentes sistemas en desarrollo.*
- *Asignar tareas de programación de los nuevos sistemas o cambios a los sistemas a los analistas.*
- *Revisar sistemas en ambiente de desarrollo antes de ponerlos en producción, procurando que su funcionamiento sea el óptimo para el usuario y según los requerimientos establecidos al inicio del proyecto y otros que surjan en el desarrollo del mismo.*
- *Actualizar cambios de sistemas realizados por analista(s) cuando éstos se encuentran en producción, procurando guardar respaldos antes de dichas actualizaciones.*
- *Gestionar reuniones con las distintas áreas en los proyectos informáticos que se estén ejecutando.*
- *Gestionar con el área de desarrollo la capacitación a usuarios en sistemas desarrollados y en otros que los usuarios requieran.*
- *Revisar y supervisar del desarrollo de proyectos cuando son realizados subcontratando servicios de terceros.*

Responsabilidad de Trabajo # 3 — 15%

Ejecutar y dar seguimiento a las acciones asignadas del Plan Estratégico Institucional (PEI) y al Plan Operativo Anual (POA) de la Gerencia, realizar todas las acciones necesarias para su cumplimiento.

Tareas Permanentes:

- *Dar seguimiento a las actividades asignadas del plan estratégico.*
- *Dar seguimiento a las actividades asignadas del plan operativo.*
- *Elaborar informe de la ejecución del plan estratégico y del plan operativo*

Responsabilidad de Trabajo # 4 — 15%

Atender y dar respuesta a los requerimientos de sistemas de las distintas dependencias de SIGET relacionado con el desarrollo, rediseño y actualización de aplicaciones.

Tareas Permanentes:

- *Llevar un control de las reuniones sostenidas con los usuarios, así como los acuerdos que se realizaron en las mismas tales como nuevos requerimientos, observaciones o cambios en el diseño de los sistemas.*
- *Brindar soporte y mantenimiento a sistemas informáticos existentes y en otros que los usuarios lo requieran*
- *Asistir a reuniones varias en las que se requiera la contraparte informática y que sea relacionada con los sistemas informáticos*
- *Gestionar el rediseño y actualización de aplicaciones existentes cuando éstos sean requeridos por los usuarios o sea necesarios realizar una actualización tecnológica en los mismos.*

Responsabilidad de Trabajo # 5 — 15%

Desarrollar informes de los diferentes sistemas en desarrollo y de informes de actividades, y tareas realizadas por los analistas.

Tareas Permanentes:

- *Elaborar documentación de las reuniones en las que se traten aspectos relacionados con los sistemas informáticos y en las que sea necesario tener un control de las mismas.*
- *Elaborar informe de actividades del área de desarrollo realizadas durante el mes, para ser presentado los primeros 6 días hábiles de cada mes a la Gerencia.*
- *Actualizar tareas realizadas para el informe mensual.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 3 de resolución de Problema: Porqué las cosas que se hacen son conocidas, pero lo que se debe hacer y cómo debe hacerse no está definido. La persona debe ser analítico, crítico, investigativo y generador ideas, recomendaciones o soluciones a los problemas identificados.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☒ PRINCIPAL (asume completa y total responsabilidad)

☐ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Maestría o Post-grado en Administración de Empresas o Sistemas Informáticos, Dirección de Proyectos o áreas afines.
Educación Superior	☒	☐	Profesional Graduado en Ingeniería o , Licenciado en Sistemas Informáticos, o equivalente de educación

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia de mínima de 5 años como Jefe en Programación y Desarrollo, Integrador de Tecnología o puestos similares.

Deseable:

- Experiencia con sistemas operativos, instalación y configuración software.
- Dominio en el manejo de herramientas para la administración de proyectos.
- Experiencia en desarrollo de sistemas, definición y formulación de proyectos.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Conocimiento de lenguaje de diagramación de sistemas UML
- Lenguaje de consultas de base de datos SQL
- Conocimiento real de al menos un lenguaje de programación.
- Técnicas de calidad de software

Deseable:

- Conocimiento y experiencia en la aplicación de leyes, reglamentos e instructivos relacionados con la naturaleza del puesto.
- Conocimiento de la metodología Project Management Institute (PMI).

Competencias. En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.

A

GERENCIAS, JEFES UNIDADES ASESORAS, JEFES DEPTO *(este grupo de comportamientos incluye al personal que desempeñan puestos con carácter de Gerencia y Jefaturas de Unidades Asesoras o Departamentos).*

APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.

Comportamientos evaluados:

1. Conoce las funciones de su puesto?
2. Demuestra dominio de conocimientos técnicos y especializados?
3. Es hábil para buscar alternativas de solución?
4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
5. En momentos de crisis los problemas los resuelve con habilidad?

CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.

6. Es experto en los conocimientos concernientes a su área de trabajo, y permanentemente se actualiza en estos y en otros temas de interés que contribuyan a alcanzar los objetivos institucionales?
7. Aplica los conceptos teóricos modernos y las mejores prácticas al desarrollo de sus actividades?
8. Realiza propuestas de mejoramiento y está abierto a valorar las propuestas de otros para optimizar el desempeño?
9. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios?
10. Posee capacidad para resolver situaciones a corto y largo plazo?

ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incrmento de eficiencia en el personal.

11. Es puntual en sus compromisos de trabajo?
12. Organiza y programa adecuadamente su trabajo?
13. Mantiene una actitud receptiva hacia la información o puntos de vista de otras personas?
14. Inspira y transmite confianza en sus relaciones interpersonales?
15. Es respetuoso y considerado con sus colaboradores?

ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).

16. Planifica sus acciones y las de su equipo de trabajo , considerando las necesidades de sus clientes (internos y/o externos)?
17. Mantiene una comunicación efectiva con el cliente (interno y/o externo) para conocer sus necesidades y su nivel de satisfacción.
18. Logra que los clientes (internos y/o externos) sientan que son lo más importante para la institución, manteniendo excelentes
19. Actua como referente interno y/o externo cuando se busca aportar soluciones o satisfacer necesidades de sus clientes?
20. Trabaja con una perspectiva de largo plazo a la hora de resolver los problemas del cliente (interno y/o externo), considerando sus impactos?

LIDERAZGO : Entendido como la habilidad necesaria para orientar la acción de equipo de trabajo en una acción determinada, inspirando los valores en acción y anticipando escenarios de desarrollo de su equipo de trabajo.

21. Lidera adecuadamente las reuniones (define agenda, establece fechas, los objetivos a discutir, controla el tiempo y asigna turnos de palabra, etc.)?
22. Fija objetivos, los transmite claramente, realiza el seguimiento y brinda coaching sobre avances?
23. Escucha y promueve la participación y la aportación de ideas?
24. Delega y empodera a su equipo transmitiendo confianza y realizando un seguimiento efectivo?
25. Tiene carisma propio, comunica una visión de futuro que genera entusiasmo y compromiso con la misión de la institución?

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización.**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes.**	Adquirir productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

Condiciones de Trabajo

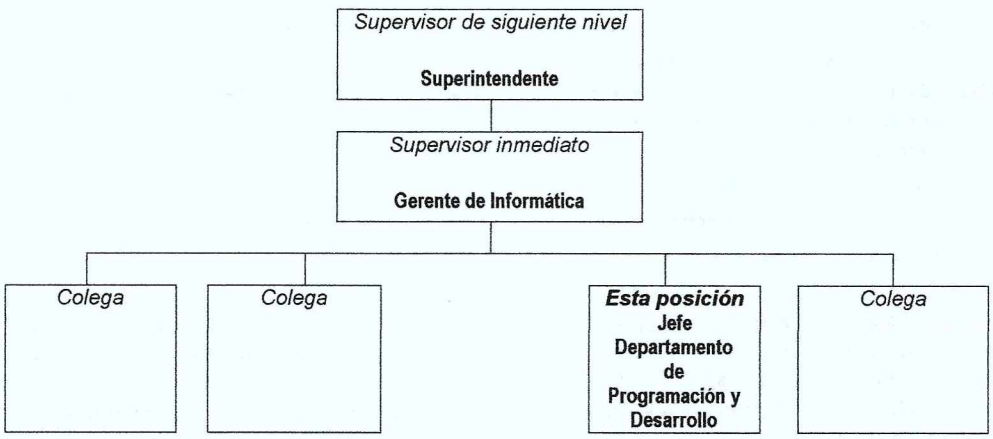
Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina **98%**

Porcentaje esperado de tiempo en viajes (al interior y exterior del país) **2%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 02

02

TÉCNICO ADMINISTRADOR DE PÁGINA WEB

Título del Puesto

GERENCIA DE INFORMÁTICA

-11-

Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

EXPERTO	-1-	AGOSTO 2017
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. ***Por qué*** *existe el puesto y* ***qué debe lograr****, recuerde que NO se requiere una lista de actividades, sino la* ***Misión principal del puesto****.*

Administrar, actualizar y desarrollar los diferentes sitios web de la institución, así como la actualización de la Intranet y participar eficientemente en el cumplimiento de los objetivos y metas de la Gerencia.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 40%

Velar por el buen funcionamiento global del sitio Institucional, verificando la disponibilidad, así como supervisar que el software funcione correctamente.

Tareas Permanentes:

- *Verificar la integridad de la información en el sitio Web periódicamente.*
- *Verificar la disponibilidad del sitio Web Institucional diariamente.*
- *Verificar que el software del sitio Web Institucional funcione de manera correcta periódicamente.*
- *Verificar el cumplimiento de los estándares establecidos por Casa Presidencial para sitios web gubernamentales.*
- *Implementar nuevas plantillas de la página web cuando sea necesario.*

Responsabilidad de Trabajo # 2 — 35%

Actualizar, administrar y dar mantenimiento al contenido de los Sitios Web de la Institución e Intranet.

Tareas Permanentes:

- *Recibir información autorizada de las diferentes Unidades y Gerencias para publicarla Web Institucional o intranet*
- *Actualizar la información publicada en el sitio Web Institucional o intranet previa autorización.*
- *Responsable del mantenimiento del sitio Web de la Institución y la intranet.*
- *Responsable del certificado de seguridad de la página web.*
- *Publicar las noticias, avisos y galería de imágenes de eventos realizados ya sea en el sitio web o intranet.*
- *Elaborar encuestas*
- *Realizar otras funciones, como creación de banner y edición de fotografías según se necesite para las publicaciones.*

Responsabilidad de Trabajo # 3 — 25%

Realizar copias de respaldo de los Sitios Web de la Institución, de manera mensual para entrega de medios para resguardo, y elaborar un informe mensual con todas las tareas realizadas para reportar a su superior.

Tareas Permanentes

- *Realizar un respaldo mensual para entrega de medios para resguardo.*
- *Realizar respaldos del sitio periódicamente.*
- *Elaborar un informe mensual con todas las tareas realizadas para reportar a su superior.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 2 de resolución de Problema: Porqué lo que hay que hacer es conocido, pero como hacerlo no está definido. La persona debe de usar habilidades de interpolación para escoger la estrategia correcta para tratar el problema dado.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☐ PRINCIPAL (asume completa y total responsabilidad)

☒ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Graduado en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.
Educación Superior	☒	☐	Cursando Tercer año en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia mínima de 3 años como técnico en administración, mantenimiento y desarrollo de páginas Web o similares.

Deseable:

- Conocimiento en administración, mantenimiento y desarrollo de páginas Web con WordPress y Joomla.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Conocimiento y Manejo de Procesadores de Texto, Excel, PowerPoint y Otros.
- Programar y desarrollar las páginas que conforman el sitio web,
- Instalar y administrar parches necesarios para el adecuado funcionamiento del sitio web;
- Conocimiento en la actualización de contenidos en las diferentes páginas que conforman el sitio Web.
- Conocimiento en la actualización y corrección de errores de ejecución en el código fuente que puedan ocasionar la no visualización de las páginas o fragmentos de ellas en los distintos sitios de la Intranet e Internet.

Deseable: Resolución de problemas lógicos, manejo básico de computadoras.

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

B

PERSONAL TECNICO Y ADMINISTRATIVO *(este grupo incluye al personal que desarrollan labores técnicas y/o Administrativas en áreas especializadas de la institución).*

APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.

Comportamientos evaluados:

1. Conoce las funciones de su puesto?
2. Demuestra dominio de conocimientos técnicos y especializados?
3. Posee capacidad propósitiva y criterio propio para solucionar las dificultades con sensatez y acudir en forma independiente y eficaz, sin necesidad de que se le proporcionen instrucciones?
4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
5. Proporciona respuestas oportunas a las exigencias de trabajo?

CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.

6. Identifica las tareas esenciales a realizar en el trabajo?
7. Se dedica a cumplir con su trabajo en el plazo establecido, evitando distraerse con asuntos personales?
8. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios al finalizarla?
9. Comprende la interrelación existente de trabajo entre su área y otras areas de la institución?.
10. Frecuentemente realiza un esfuerzo mas allá de lo normal, para dar por finalizada una tarea asignada o problemas especificos?

ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incrmento de eficiencia en el personal.

11. Es puntual en sus compromisos de trabajo?
12. Organiza y programa adecuadamente su trabajo?
13. Sabe como trabajar formando parte de un equipo?
14. Inspira y transmite confianza en sus relaciones interpersonales?
15. Es respetuoso y considerado con sus superiores y compañeros de trabajo?

ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).

16. Entiende con facilidad los problemas y/o necesidades de sus clientes (internos y/o externos)?
17. Desarrolla soluciones a los problemas de los clientes (internos y/o externos), trabajando junto con ellos?
18. Asesora y da al cliente (interno y/o externo) las alternativas que mejor se adaptan a sus necesidades?
19. Se apega a los tiempos estipulados para la entrega de los servicios solicitados por los clientes (internos y/o externos), exigiéndose cumplir en tiempo y calidad?
20. Hace más de lo que normalmente el cliente (nterno y/o externo) espera?

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes**	Para adquisiciones de productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

Condiciones de Trabajo

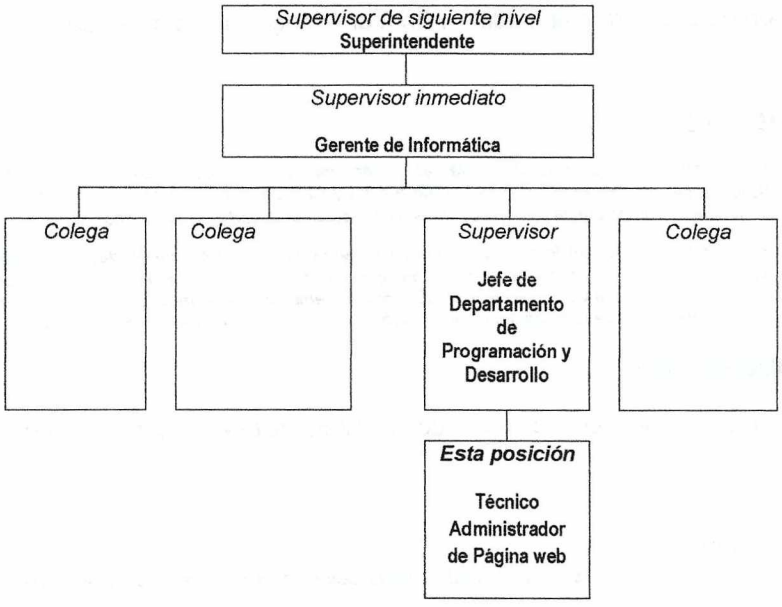
Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina **100%**

Porcentaje esperado de tiempo en viajes (al interior y exterior del país) **-- %**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 02

03

TÉCNICO DE PROGRAMACIÓN Y DESARROLLO

Título del Puesto

GERENCIA DE INFORMÁTICA

-11-

Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

EXPERTO	**-2-**	**AGOSTO 2017**
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. ***Por qué*** *existe el puesto y* ***qué debe lograr****, recuerde que NO se requiere una lista de actividades, sino la* ***Misión principal del puesto****.*

Satisfacer los requerimientos de las Gerencias y Unidades de SIGET, a través del análisis, diseño, desarrollo e implementación de software a la medida y brindar el seguimiento del buen funcionamiento de los mismos.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 35%

Encargado de la fase de planificación que comprende analizar, diseñar y crear la documentación del requerimiento.

Tareas Permanentes:

- *Recibir la definición de los requerimientos.*
- *Crear documento de diseño en base a los requerimientos de la solución propuesta si esta no fuera entregada por su Superior.*
- *Crear la documentación adicional necesaria para cumplir con el requerimiento.*

Responsabilidad de Trabajo # 2 — 30%

Crear la Base de Datos y/o codificación de los diferentes módulos del sistema, creación de archivos compilados e instalar y ejecutar la solución en un ambiente desarrollado; la documentación y presentación de avances al supervisor inmediato.

Tareas Permanentes:

- *Crear la Base de Datos*
- *Codificar los módulos*
- *Crear archivos compilados*
- *Instalar y ejecutar la solución en un ambiente desarrollado*
- *Documentar y presentar avances.*

Responsabilidad de Trabajo # 3 — 20%

Encargado de ambientes de producción: Definir las condiciones o requisitos bajo las cuales el sistema desarrollado se ejecutara correctamente en un ambiente de producción donde será instalado.

Tareas Permanentes:

- *Crear el documento técnico del software donde se detalle los procesos lógicos implementados, el modelo de la base de datos, las reglas de instalación y configuración, controles de auditoria, etc.*
- *Instalar la solución en un ambiente de producción;*
- *Crear manuales Técnicos y de Usuarios;*
- *Capacitar al personal que hará uso de la solución*

Responsabilidad de Trabajo # 4 — 15%

Asistir a los usuarios en la corrección o modificación de registros en la base de datos generados por uso no adecuado de las aplicaciones.

Tareas Permanentes:

- *Asistir a usuarios sobre el uso de los sistemas desarrollados;*
- *Realizar correctivos de datos por mal uso de las aplicaciones;*
- *Realizar mantenimiento correctivo de los programas.*
- *Documentar en los formatos designados los soportes brindados a los usuarios;*
- *Describir las actividades de trabajo diarias, el tiempo invertido y porcentaje de avances en cada actividad;*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 2 de resolución de Problema: Porqué lo que hay que hacer es conocido, pero como hacerlo no está definido. La persona debe de usar habilidades de interpolación para escoger la estrategia correcta para tratar el problema dado.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☐ PRINCIPAL (asume completa y total responsabilidad)

☒ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Graduado en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.
Educación Superior	☒	☐	Cursando Tercer año en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia mínima de 3 años como Técnico Programador o Informático en Sistemas.

Deseable:

- Experiencia progresiva de carácter operativo en el área de programación y manejo de programas.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Capacidad de análisis y síntesis.
- Conocimiento y Manejo de Procesadores de Texto, Excel, PowerPoint y Otros.
- Capacidad para trabajar en equipos multidisciplinarios.
- Buenas relaciones interpersonales
- Métodos y herramientas actualizadas para el análisis y desarrollo de sistemas de información.
- Sistemas operativos.
- Inglés intermedio.
- Mantenimiento de software y/o hardware.
- Lenguajes de programación.
- Manejo de bases de datos.

Deseable:

Manejo de equipos y herramientas de computación.

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

PERSONAL TECNICO Y ADMINISTRATIVO *(este grupo incluye al personal que desarrollan labores técnicas y/o Administrativas en áreas especializadas de la institución).*

APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.

Comportamientos evaluados:

1. Conoce las funciones de su puesto?
2. Demuestra dominio de conocimientos técnicos y especializados?
3. Posee capacidad propósitiva y criterio propio para solucionar las dificultades con sensatez y acudir en forma independiente y eficaz, sin necesidad de que se le proporcionen instrucciones?
4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
5. Proporciona respuestas oportunas a las exigencias de trabajo?

CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.

6. Identifica las tareas esenciales a realizar en el trabajo?
7. Se dedica a cumplir con su trabajo en el plazo establecido, evitando distraerse con asuntos personales?
8. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios al finalizarla?
9. Comprende la interrelación existente de trabajo entre su área y otras areas de la institución?.
10. Frecuentemente realiza un esfuerzo mas allá de lo normal, para dar por finalizada una tarea asignada o problemas especificos?

ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incremento de eficiencia en el personal.

11. Es puntual en sus compromisos de trabajo?
12. Organiza y programa adecuadamente su trabajo?
13. Sabe como trabajar formando parte de un equipo?
14. Inspira y transmite confianza en sus relaciones interpersonales?
15. Es respetuoso y considerado con sus superiores y compañeros de trabajo?

ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).

16. Entiende con facilidad los problemas y/o necesidades de sus clientes (internos y/o externos)?
17. Desarrolla soluciones a los problemas de los clientes (internos y/o externos), trabajando junto con ellos?
18. Asesora y da al cliente (interno y/o externo) las alternativas que mejor se adaptan a sus necesidades?
19. Se apega a los tiempos estipulados para la entrega de los servicios solicitados por los clientes (internos y/o externos), exigiéndose cumplir en tiempo y calidad?
20. Hace más de lo que normalmente el cliente (nterno y/o externo) espera?

B

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Institución**	Cumplir con las solicitudes de requerimientos de nuevos sistemas o mejoras de estos, facilitar la apuesta en marcha de las soluciones a los sistemas informáticos, de acuerdo a prioridades establecidas.
Externos	**Proveedores de servicios y bienes**	Adquisiciones de productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

Condiciones de Trabajo

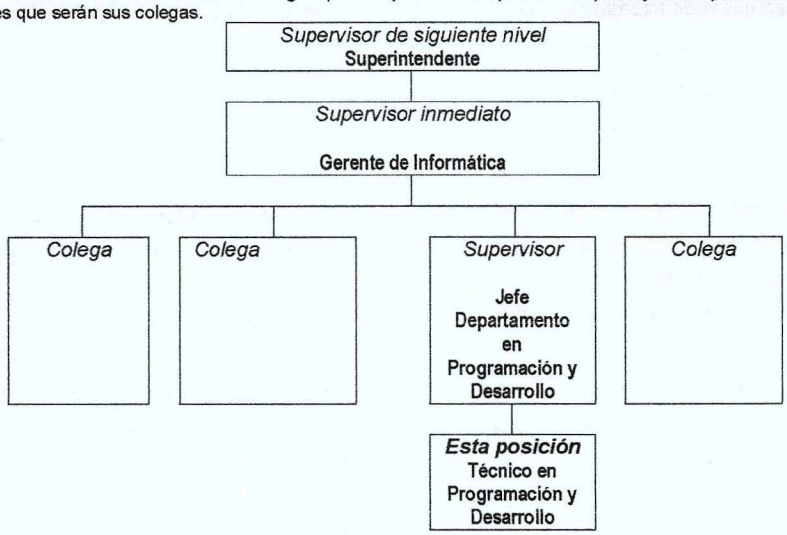
Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina **100%**

Porcentaje esperado de tiempo en viajes (al interior y exterior del país) **-- %**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 03 DEPARTAMENTO DE ADMINISTRACIÓN DE RED Y SOPORTE A USUARIOS.

01

JEFE DE DEPARTAMENTO DE ADMINISTRACIÓN DE RED Y SOPORTE A USUARIOS

Título del Puesto

GERENCIA DE INFORMÁTICA

Gerencia /Unidad Asesora/Jefatura Técnica

-16-
Grado/Nivel Puesto

JEFE	**-1-**	**AGOSTO 2017**
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. ***Por qué*** *existe el puesto y* ***qué debe lograr****, recuerde que NO se requiere una lista de actividades, sino la* ***Misión principal del puesto****.*

Administrar el uso efectivo de los equipos informáticos, redes de comunicación y el respaldo de la información institucional, participar eficientemente en el cumplimiento de los objetivos y metas de la Gerencia.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 25%

Supervisar y apoyar al personal en la asignación de actividades, medir los objetivos asignados a cada persona y el desempeño de sus actividades o deberes, mediante evaluaciones de desempeño y cumplimientos de objetivos logrados, sugerir capacitaciones orientadas al mejoramiento continuo de las capacidades del personal.

Tareas Permanentes:

- *Asignar actividades a los empleados a su cargo.*
- *Medir los objetivos asignados a los empleados a su cargo.*
- *Manejar el desempeño del personal a su cargo.*
- *Acompañar las actividades y deberes de los empleados.*
- *Coordinar las evaluaciones de personal a su cargo.*

- *Sugerir acciones de capacitación orientadas al mejoramiento continuo de las capacidades del personal a su cargo.*

Responsabilidad de Trabajo # 2 — 15%

Ejecutar y dar seguimiento a las acciones asignadas del Plan Estratégico Institucional (PEI) y al Plan Operativo Anual (POA) de la Gerencia, realizar todas las acciones necesarias para su cumplimiento.

Tareas Permanentes:

- *Dar seguimiento a las actividades asignadas del plan estratégico.*
- *Dar seguimiento a las actividades asignadas del plan operativo.*
- *Elaborar informe de la ejecución del plan estratégico y del plan operativo.*

Responsabilidad de Trabajo # 3 — 15%

Planificar la organización y configuración de la red de todas las configuraciones físicas y lógicas con sus respaldos, determinar los recursos que utilizara, y la debida documentación de los cambios realizados, la administración de los servidores y equipos de red tanto en hardware y software, así como la instalación y prueba de equipo nuevo que se adquiera en la Gerencia de Informática.

Tareas Permanentes:

- *Planificar la organización de la red, determinar los recursos que utilizara y donde se localiza.*
- *Documentar la configuración de la red y los cambios realizados incluyendo topologías de red y bitácoras de cambios.*
- *Administrar los servidores y otros equipos periféricos de la red tanto en hardware y software*
- *Coordinar y revisar las instalaciones y pruebas de todo equipo nuevo que se adquiera en la Gerencia de Informática.*
- *Encargado de recomendar que equipos comprar.*
- *Seguimiento de la administración de la planta telefónica.*

Responsabilidad de Trabajo # 4 — 5%

Detectar y corregir fallas que ocurran en la red, y establecer medidas preventivas y correctivas con antelación y definir un plan de contingencia en caso de emergencia, coordinación de planes de mantenimiento preventivo, correctivo, monitoreo y control de tráfico de red de datos.

Tareas Permanentes:

- *Detectar y solucionar los problemas que ocurran con la red.*
  Establecer medidas preventivas y correctivas con antelación.
- *Definir un plan de contingencia en caso de emergencia.*
- *Coordinar planes de mantenimiento preventivo, correctivo y monitoreo de equipos de red de datos*
- *Monitorear y controlar el tráfico de la red y las operaciones que en ella se efectúen.*
- *Coordinar servicios de soporte o mantenimiento relacionados a la red brindados por terceros.*

Responsabilidad de Trabajo # 5 — 10%

Administrar y establecer medidas de seguridad física como seguridad lógica de la red y podrá apoyarse en el Jefe de Seguridad de la Información, habilitar acceso a los recursos de la red, como los hosts, los dispositivos y los archivos según se soliciten y autorice, el establecimiento de la seguridad de la red inalámbrica y a los accesos remotos hacia la red; y respaldos establecidos dentro del plan de contingencia.

Tareas Permanentes:

- *Establecer medidas de seguridad física y lógica.*
- *Habilitar acceso a los recursos de la red, como los hosts, los dispositivos y los archivos según se solicite y autorice.*
- *Establecer la seguridad de la red inalámbrica y a los accesos remotos hacia la red.*
- *Realizar respaldos establecidos dentro del plan de contingencia.*
- *Seguimiento de la administración de software.*
- *Encargado del centro de datos institucional y el equipo en él.*

Responsabilidad de Trabajo # 6 — 5%

Coordinar planes de mantenimiento a los equipos: mantenimientos preventivos, correctivos y monitoreo entre otros necesarios.

Tareas Permanentes:

- *Establecer calendarios de mantenimiento a los equipos de usuarios finales.*
- *Llevar control de la ejecución de los mantenimientos.*
- *Asignar los recursos de personal de la Gerencia de informática para realizar dichos mantenimientos y los insumos para realizarlos.*
- *Coordinar los mantenimientos si los servicios han sido subcontratados.*
- *Establecer los mantenimientos básicos para cada tipo de equipo según sus características.*

Responsabilidad de Trabajo # 7 — 10%

Coordinación de soporte a usuarios: brindar soporte a los usuarios de la institución y elaborar estadísticas de incidencias.

Tareas Permanentes:

- *Responsable de revisar las incidencias para soportes*
- *Asignará los soportes a los empleados a su cargo para realizar los soportes*
- *Dar seguimiento a la resolución de problemas*
- *Elaborar un informe mensual de los soportes realizados por el personal a su cargo.*

Responsabilidad de Trabajo # 8 — 15%

Administración de software y hardware: relacionados a los niveles de estaciones de usuarios finales.

Tareas Permanentes:

- *Control de licencias y uso de programas informáticos a nivel de estaciones de usuarios finales.*
- *Administrar las actualizaciones de sistemas, programas a nivel de estaciones de usuarios finales.*
- *Dar seguimiento a los movimientos de equipo realizados por personal de la Gerencia de Informática según los procedimientos establecidos por el encargado de inventario institucional.*
- *Responsable del control de activos de equipos, materiales de reparación y limpieza que se guarden en la Gerencia de Informática y bodega de informática.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 3 de resolución de Problema: Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. La persona debe ser analítico, crítico, investigativo y generador ideas, recomendaciones o soluciones a los problemas identificados.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☒ PRINCIPAL (asume completa y total responsabilidad)

☐ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Maestría o Post-grado en Administración de Redes o Computación, Seguridad Informática o áreas afines.
Educación Superior	☒	☐	Profesional Graduado en Ingeniería o , Licenciado en Sistemas Informáticos, o equivalente de educación

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

A	GERENCIAS, JEFES UNIDADES ASESORAS, JEFES DEPTO *(este grupo de comportamientos incluye al personal que desempeñan puestos con carácter de Gerencia y Jefaturas de Unidades Asesoras o Departamentos).*
	APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.
	Comportamientos evaluados:
	1. Conoce las funciones de su puesto?
	2. Demuestra dominio de conocimientos técnicos y especializados?
	3. Es hábil para buscar alternativas de solución?
	4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
	5. En momentos de crisis los problemas los resuelve con habilidad?
	CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.
	6. Es experto en los conocimientos concernientes a su área de trabajo, y permanentemente se actualiza en estos y en otros temas de interés que contribuyan a alcanzar los objetivos institucionales?
	7. Aplica los conceptos teóricos modernos y las mejores prácticas al desarrollo de sus actividades?
	8. Realiza propuestas de mejoramiento y está abierto a valorar las propuestas de otros para optimizar el desempeño?
	9. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios?
	10. Posee capacidad para resolver situaciones a corto y largo plazo?
	ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incremento de eficiencia en el personal.
	11. Es puntual en sus compromisos de trabajo?
	12. Organiza y programa adecuadamente su trabajo?
	13. Mantiene una actitud receptiva hacia la información o puntos de vista de otras personas?
	14. Inspira y transmite confianza en sus relaciones interpersonales?
	15. Es respetuoso y considerado con sus colaboradores?
	ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).
	16. Planifica sus acciones y las de su equipo de trabajo , considerando las necesidades de sus clientes (internos y/o externos)?
	17. Mantiene una comunicación efectiva con el cliente (interno y/o externo) para conocer sus necesidades y su nivel de satisfacción.
	18. Logra que los clientes (internos y/o externos) sientan que son lo más importante para la institución, manteniendo excelentes
	19. Actua como referente interno y/o externo cuando se busca aportar soluciones o satisfacer necesidades de sus clientes?
	20. Trabaja con una perspectiva de largo plazo a la hora de resolver los problemas del cliente (interno y/o externo), considerando sus impactos?
	LIDERAZGO : Entendido como la habilidad necesaria para orientar la acción de equipo de trabajo en una acción determinada, inspirando los valores en acción y anticipando escenarios de desarrollo de su equipo de trabajo.
	21. Lidera adecuadamente las reuniones (define agenda, establece fechas, los objetivos a discutir, controla el tiempo y asigna turnos de palabra, etc.)?
	22. Fija objetivos, los transmite claramente, realiza el seguimiento y brinda coaching sobre avances?
	23. Escucha y promueve la participación y la aportación de ideas?
	24. Delega y empodera a su equipo transmitiendo confianza y realizando un seguimiento efectivo?
	25. Tiene carisma propio, comunica una visión de futuro que genera entusiasmo y compromiso con la misión de la institución?

Experiencia **Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.**

Requerida:

- Experiencia mínima de 5 años como Jefe en Administración de Red, Soporte de Informática o puestos similares.

Deseable:

- Experiencia con sistemas operativos
- Configuración de redes
- Configuración de bases de datos,
- Configuración de hardware y software.

Habilidades Técnicas **Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:**

Requerida:

- Idioma ingles técnico, a nivel intermedio.
- En administración de redes y sistemas de almacenamiento masivo.
- Sistemas de control de usuarios y correo.

Deseable:

- Amplio conocimiento en informática y telecomunicaciones
- Conocimiento y experiencia en la aplicación de leyes, reglamentos e instructivos relacionados con la naturaleza del puesto.

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes**	Adquirir productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

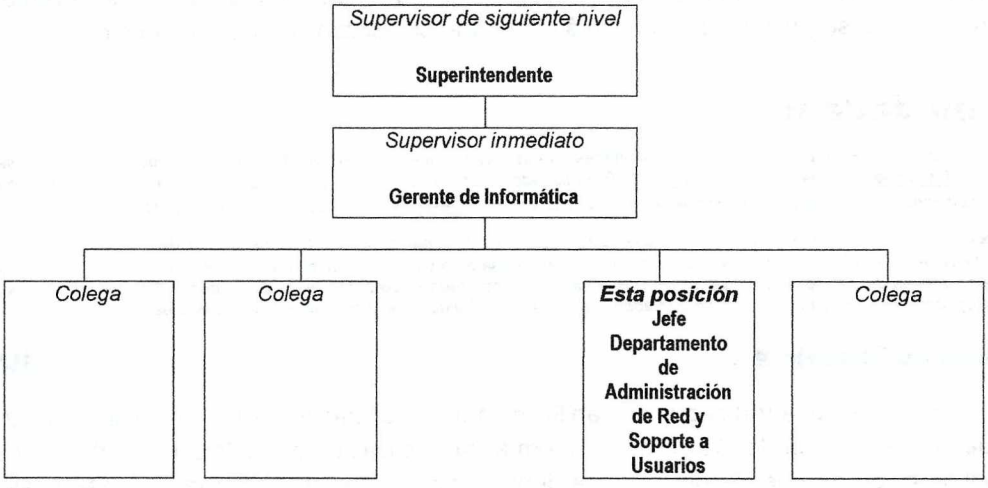
Condiciones de Trabajo

Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina	**90%**
Porcentaje esperado de tiempo en viajes (al interior y exterior del país)	**10%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 03

02

TÉCNICO EN ADMINISTRACIÓN DE RED

Título del Puesto

GERENCIA DE INFORMÁTICA

-11-

Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

EXPERTO	**-1-**	**AGOSTO 2017**
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. ***Por qué*** *existe el puesto y* ***qué debe lograr****, recuerde que NO se requiere una lista de actividades, sino la* ***Misión principal del puesto****.*

Ejecutar medidas preventivas y correctivas sobre fallas en la red de datos; realizar mantenimientos de equipo y monitoreo y en la seguridad de la red inalámbrica y a los accesos remotos de la red.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 30%

Ejecutar las configuraciones de la red según la planificación de organización de red, instalar y probar todo equipo nuevo que se adquiera en la Gerencia de Informática, realización de instalaciones de cableados, verificación y configuración de puertos de red, y la debida documentación de las tareas realizadas para repórtalos al superior inmediato.

Tareas Permanentes:

- *Ejecutar las configuraciones de la red según la planificación de organización de red.*
- *Realizar respaldo de las configuraciones de los equipos.*
- *Instalar y probar todo equipo nuevo que se adquiera en la Gerencia de Informática.*
- *Realizar instalaciones de cableados, verificación y configuración de puertos de red.*
- *Documentar las tareas realizados para reportarlos a su superior.*

Responsabilidad de Trabajo # 2 — 25%

Ejecutar medidas preventivas y correctivas sobre fallas en la red de datos, y realizar mantenimientos de equipo, monitoreo y la supervisión de servicios de soporte o mantenimiento brindados por terceros.

Tareas Permanentes:

- *Brindar soporte en sitio en los casos que fuera necesario.*
- *Ejecutar medidas preventivas y correctivas sobre fallas en la red de datos.*
- *Realizar mantenimientos de equipo y monitoreo.*
- *Supervisar servicios de soporte o mantenimiento brindados por terceros.*
- *Solicitar soporte a proveedores y gestionar garantías.*
- *Apoyar la puesta en marcha de los planes de contingencia establecidos.*

Responsabilidad de Trabajo # 3 — 15%

Configurar los accesos a los recursos de la red, como los hosts, los dispositivos y los archivos según indique su superior y dar seguimiento a la seguridad de la red inalámbrica y a los accesos remotos hacia la red.

Tareas Permanentes:

- *Apoyar en las implementaciones de medidas de seguridad física y lógica.*
- *Configurar los accesos a los recursos de la red, como los hosts, los dispositivos y los archivos según indique su superior.*
- *Dar seguimiento a la seguridad de la red inalámbrica y a los accesos remotos hacia la red.*
- *Realizar respaldos establecidos dentro del plan de contingencia.*
- *Llevar el control de ingresos a centro de datos.*

Responsabilidad de Trabajo # 4 — 20%

Realizar la Administración de software, y control de licencias y uso de programas informáticos a nivel de servidores y servicios así mismo administrar las actualizaciones de sistemas, programas a nivel de servidores y servicios.

Tareas Permanentes:

- *Control de licencias y uso de programas informáticos a nivel de servidores y servicios.*
- *Administrar las actualizaciones de sistemas, programas a nivel de servidores y servicios.*
- *Documentar todas las tareas relacionadas.*
- *Recomendar a su superior actualizaciones y parches al software.*

Responsabilidad de Trabajo # 5 — 10%

Realizar cambios, configuraciones, actualizaciones y administración de la planta telefónica.

Tareas Permanentes:

- *Realizar cambios y configuraciones en la planta telefónica.*
- *Realizar actualización a la planta y copias de seguridad.*
- *Supervisar servicios de soporte o mantenimiento brindados por terceros.*
- *Solicitar soporte a proveedores y gestionar garantías.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 2 de resolución de Problema: Porqué lo que hay que hacer es conocido, pero como hacerlo no está definido. La persona debe de usar habilidades de interpolación para escoger la estrategia correcta para tratar el problema dado.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☐ PRINCIPAL (asume completa y total responsabilidad)

☒ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Título Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Graduado en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.
Educación Superior	☒	☐	Cursando Tercer año en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

PERSONAL TECNICO Y ADMINISTRATIVO *(este grupo incluye al personal que desarrollan labores técnicas y/o Administrativas en áreas especializadas de la institución).*

APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.

Comportamientos evaluados:

1. Conoce las funciones de su puesto?
2. Demuestra dominio de conocimientos técnicos y especializados?
3. Posee capacidad propósitiva y criterio propio para solucionar las dificultades con sensatez y acudir en forma independiente y eficaz, sin necesidad de que se le proporcionen instrucciones?
4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
5. Proporciona respuestas oportunas a las exigencias de trabajo?

CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, así como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.

6. Identifica las tareas esenciales a realizar en el trabajo?
7. Se dedica a cumplir con su trabajo en el plazo establecido, evitando distraerse con asuntos personales?
8. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios al finalizarla?
9. Comprende la interrelación existente de trabajo entre su área y otras areas de la institución?.
10. Frecuentemente realiza un esfuerzo mas allá de lo normal, para dar por finalizada una tarea asignada o problemas especificos?

ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incrmento de eficiencia en el personal.

11. Es puntual en sus compromisos de trabajo?
12. Organiza y programa adecuadamente su trabajo?
13. Sabe como trabajar formando parte de un equipo?
14. Inspira y transmite confianza en sus relaciones interpersonales?
15. Es respetuoso y considerado con sus superiores y compañeros de trabajo?

ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).

16. Entiende con facilidad los problemas y/o necesidades de sus clientes (internos y/o externos)?
17. Desarrolla soluciones a los problemas de los clientes (internos y/o externos), trabajando junto con ellos?
18. Asesora y da al cliente (interno y/o externo) las alternativas que mejor se adaptan a sus necesidades?
19. Se apega a los tiempos estipulados para la entrega de los servicios solicitados por los clientes (internos y/o externos), exigiéndose cumplir en tiempo y calidad?
20. Hace más de lo que normalmente el cliente (nterno y/o externo) espera?

B

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia de 3 años como Técnico en administración de redes o en puestos similares

Deseable:

- Experiencia con sistemas operativos, redes, bases de datos, configuración de hardware y software.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Idioma ingles a nivel intermedio.
- En administración de redes y sistemas de almacenamiento masivo.
- Sistemas de control de usuarios y correo
- Cableado estructurado y protocolos de internet

Deseable:

- Conocimiento en reparación de equipos.

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes**	Adquirir productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

Condiciones de Trabajo

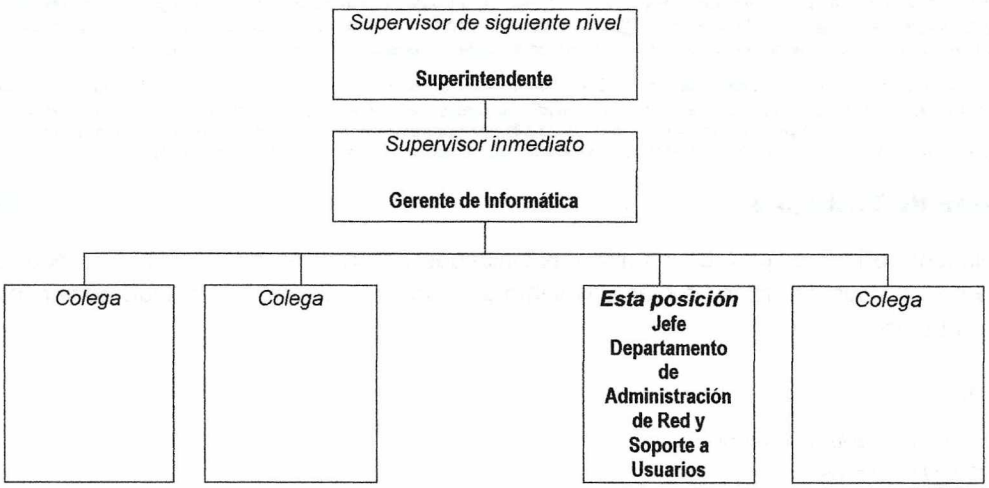
Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina **98%**

Porcentaje esperado de tiempo en viajes (al interior y exterior del país) **2%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 03

03

TÉCNICO DE SOPORTE A USUARIOS

Título del Puesto

GERENCIA DE INFORMÁTICA

-11-

Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

EXPERTO	-4-	AGOSTO 2017
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

*En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. **Por qué** existe el puesto y **qué debe lograr**, recuerde que NO se requiere una lista de actividades, sino la **Misión principal del puesto**.*

Brindar soporte a los usuarios, instalar software, realizar configuraciones y reparaciones de estaciones de trabajo, entre otros apoyos técnicos que se necesiten.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 35%

Realizar mantenimiento a los equipos, de las distintas Unidades y Gerencias de la Institución, acompañar al personal de terceros si los servicios de mantenimiento son subcontratados; y la debida documentación de los mantenimientos realizados.

Tareas Permanentes:

- *Verificar las rutinas para los mantenimientos.*
- *Realizar los mantenimientos.*
- *Acompañar al personal de terceros si los servicios de mantenimiento son subcontratados.*
- *Documentar los mantenimientos realizados.*

Responsabilidad de Trabajo # 2 — 25%

Ejecutar los soportes a usuarios durante el día, según solicitudes asegurándose de su finalización de forma satisfactoria, realizar inducciones sobre uso de equipos y software, el reporte de fallas de equipos que cuenten con soporte subcontratado y dar seguimiento a su reparación; y la debida documentación de los soportes y tareas realizadas.

Tareas Permanentes:

- *Verificar las asignaciones de soportes a usuarios durante el día.*
- *Realizar los soportes según solicitudes asegurándose de su finalización de forma satisfactoria.*
- *Realizar inducciones sobre uso de equipos y software a los usuarios.*
- *Reportar fallas de equipos que cuenten con soporte subcontratado y dar seguimiento a su reparación.*
- *Documentar los soportes y tareas realizados.*

Responsabilidad de Trabajo # 3 — 25%

Instalar y configurar las licencias de programas informáticos a nivel de estaciones de usuarios finales, así como la instalación y verificación de actualizaciones de sistemas, reparaciones de usuario, apoyo en instalaciones de licencias por servicios subcontratados, y configuraciones de impresoras y otros equipos de escritorio.

Tareas Permanentes:

- *Instalar y configurar las licencias y de programas informáticos a nivel de estaciones de usuarios finales.*
- *Instalar y verificar las actualizaciones de sistemas, programas a nivel de estaciones de usuarios finales.*
- *Crear las fichas de los movimientos de equipo realizados por personal de la Gerencia de Informática.*
- *Realizar reparaciones de usuarios.*
- *Apoyar en instalaciones de licencias por servicios subcontratados.*
- *Configurar impresoras y otros equipos de escritorio.*

Responsabilidad de Trabajo # 4 — 15%

Brindar soporte a los usuarios en los sistemas institucionales, brindar inducciones sobre el uso de los sistemas y proporcionar manuales de usuarios, realizar soportes relacionados a los sistemas y dar reporte, solución y seguimiento a fallas de usos de los sistemas como errores de ingreso para remitirlo al área de desarrollo.

Tareas Permanentes:

- *Habilitar el uso de recursos de los sistemas.*
- *Brindar inducciones sobre el uso de los sistemas y proporcionar manuales de usuarios.*
- *Apoyar en el primer uso de los sistemas institucionales a los usuarios.*
- *Realizar soportes relacionados a los sistemas.*
- *Reportar, solucionar y dar seguimiento a fallas de usos de los sistemas como errores de ingreso para remitirlo al área de desarrollo.*
- *Documentar las tareas realizadas.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 2 de resolución de Problema: Porqué lo que hay que hacer es conocido, pero como hacerlo no está definido. La persona debe de usar habilidades de interpolación para escoger la estrategia correcta para tratar el problema dado.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☐ PRINCIPAL (asume completa y total responsabilidad)

☒ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Graduado en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.
Educación Superior	☒	☐	Cursando Tercer año en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia mínima de 3 años como Técnico en Mantenimiento de Computadoras, Soporte a Usuarios.

Deseable:

- Experiencia con sistemas operativos, redes, bases de datos, configuración de hardware y software.
- Mantenimiento de equipos.
- Mesas de servicio.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Conocimiento y Manejo de Procesadores de Texto, Excel, PowerPoint y Otros.
- Ejecutar medidas preventivas y correctivas sobre fallas en los equipos informáticos.
- Realizar mantenimientos de equipo y monitoreo;
- Sistemas de control de usuarios y correo.

Deseable:

- Certificaciones en mantenimiento de equipos o Redes y Cableado.

Competencias.

En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.

	PERSONAL TECNICO Y ADMINISTRATIVO *(este grupo incluye al personal que desarrollan labores técnicas y/o Administrativas en áreas especializadas de la institución).*
B	**APTITUDES PERSONALES:** Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.
	Comportamientos evaluados:
	1. Conoce las funciones de su puesto?
	2. Demuestra dominio de conocimientos técnicos y especializados?
	3. Posee capacidad propósitiva y criterio propio para solucionar las dificultades con sensatez y acudir en forma independiente y eficaz, sin necesidad de que se le proporcionen instrucciones?
	4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
	5. Proporciona respuestas oportunas a las exigencias de trabajo?
	CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.
	6. Identifica las tareas esenciales a realizar en el trabajo?
	7. Se dedica a cumplir con su trabajo en el plazo establecido, evitando distraerse con asuntos personales?
	8. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios al finalizarla?
	9. Comprende la interrelación existente de trabajo entre su área y otras areas de la institución?.
	10. Frecuentemente realiza un esfuerzo mas allá de lo normal, para dar por finalizada una tarea asignada o problemas especificos?
	ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incremento de eficiencia en el personal.
	11. Es puntual en sus compromisos de trabajo?
	12. Organiza y programa adecuadamente su trabajo?
	13. Sabe como trabajar formando parte de un equipo?
	14. Inspira y transmite confianza en sus relaciones interpersonales?
	15. Es respetuoso y considerado con sus superiores y compañeros de trabajo?
	ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).
	16. Entiende con facilidad los problemas y/o necesidades de sus clientes (internos y/o externos)?
	17. Desarrolla soluciones a los problemas de los clientes (internos y/o externos), trabajando junto con ellos?
	18. Asesora y da al cliente (interno y/o externo) las alternativas que mejor se adaptan a sus necesidades?
	19. Se apega a los tiempos estipulados para la entrega de los servicios solicitados por los clientes (internos y/o externos), exigiéndose cumplir en tiempo y calidad?
	20. Hace más de lo que normalmente el cliente (nterno y/o externo) espera?

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización.**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes**	Adquirir productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

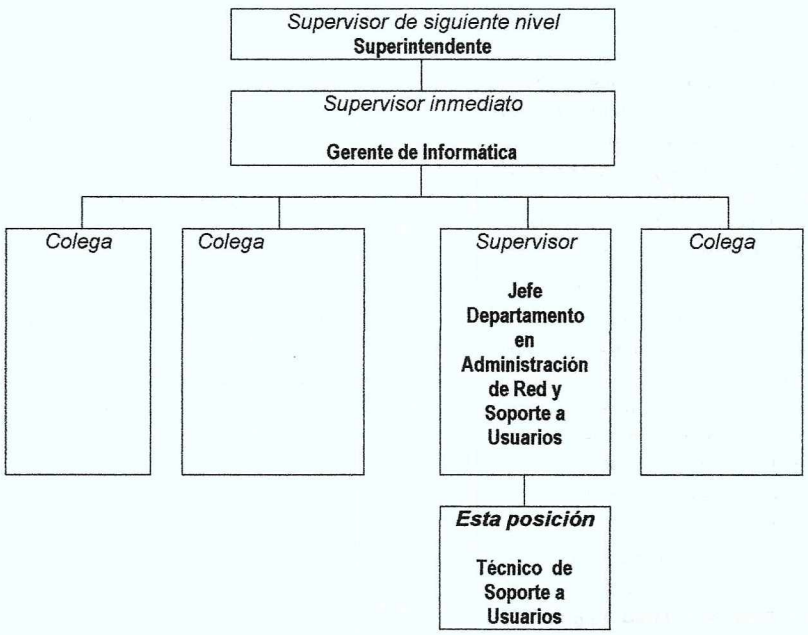
Condiciones de Trabajo

Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina	**90%**
Porcentaje esperado de tiempo en viajes (al interior y exterior del país)	**10%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 04 DEPARTAMENTO EN SEGURIDAD INFORMÁTICA

01

JEFE DE DEPARTAMENTO EN SEGURIDAD INFORMÁTICA

Título del Puesto

GERENCIA DE INFORMÁTICA

-16-

Grado/Nivel Puesto

Gerencia /Unidad Asesora/Jefatura Técnica

JEFE	-1-	AGOSTO 2017
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

*En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. **Por qué** existe el puesto y **qué debe lograr**, recuerde que NO se requiere una lista de actividades, sino la **Misión principal del puesto**.*

Proveer un marco de metodología y estandarización de la seguridad de información a la organización y sus proyectos, detectando en forma temprana causas de desvíos, implementando y administrando políticas y normativas de seguridad de la informática.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 30%

Supervisión de personal: asignación de actividades al personal a su cargo, medir los objetivos asignados a cada persona y el desempeño de sus actividades o deberes, mediante evaluaciones de desempeño y cumplimientos de objetivos logrados, sugerir capacitaciones orientadas al mejoramiento continuo de las capacidades del personal.

Tareas Permanentes:

- *Encargado de asignar actividades a los empleados a su cargo.*
- *Medir los objetivos asignados a los empleados a su cargo.*
- *Manejo del desempeño.*
- *Acompañamiento en el curso de las actividades y deberes de los empleados.*
- *Encargado de coordinar las evaluaciones de personal a su cargo*
- Encargado de sugerir acciones de capacitación orientadas al mejoramiento continuo de las capacidades del personal a su cargo.

Responsabilidad de Trabajo # 2 — 20%

Ejecutar y dar seguimiento a las acciones asignadas del Plan Estratégico Institucional (PEI) y al Plan Operativo Anual (POA) de la Gerencia, y elaborar informe de la ejecución del Plan Estratégico y del Plan Operativo.

Tareas Permanentes:

- *Dar seguimiento a las actividades asignadas del plan estratégico.*
- *Dar seguimiento a las actividades asignadas del plan operativo.*
- *Elaborar informe de la ejecución del plan estratégico y del plan operativo.*

Responsabilidad de Trabajo # 3 — 25%

Gestionar la seguridad de la información, aplicando las normativas y estándares, guiando a la misma en la implementación de políticas de seguridad y en la implementación de controles de seguridad, alineando las actividades en el marco de los estándares existentes y aplicables.

Tareas Permanentes:

- *Desarrollar e implementar las políticas y procedimientos de seguridad. Monitorear su cumplimiento.*
- *Gestionar incidentes y riesgos para garantizar la continuidad del negocio, protegiendo los activos críticos.*
- *Aplicar las metodologías, tecnologías y herramientas que existen en las distintas áreas involucradas, como ser criptografía, modelos formales, análisis forense, etc., así como en las áreas en las que la seguridad informática tiene su aplicación: redes, sistemas operativos, aplicaciones.*

Responsabilidad de Trabajo # 4 — 10%

Establecer rutinas de seguridad y las guías de implementación de la mismas en institución para ser ejecutadas el personal técnico que se encuentra bajo su cargo.

Tareas Permanentes:

- *Desarrollar periódicamente tareas de pentest (penetration testing) y todo tipo de ataque ético (Ethical Hacking) con el fin de identificar y medir vulnerabilidades para luego gestionar soluciones.*
- *Establecer un plan de Disaster Recovery (estrategia de recuperación ante desastres)*
- *Establecer un plan de contingencia para suministros de energía interrumpidos.*
- *Realizar análisis de riesgos en nuevas tecnologías*
- *Asistir a los desarrolladores en la solución de vulnerabilidades.*
- *Disuadir, Detectar y Responder a incidentes de seguridad física.*
- *Realizar actividades de gestión de riesgos (planificación, detección, mitigaciones).*
- *Alinear las actividades programadas al marco de los estándares existentes (ISO 27001, COBIT, ISAE3402, SOX, otras).*

Responsabilidad de Trabajo # 5 — 10%

Encargado de monitorear noticias y medios: relacionados a Seguridad de la Información en cuanto a temas relacionados a ataques cibernéticos, vulnerabilidades de equipos, plataformas u otros similares para evitar repercusiones en la institución.

Tareas Permanentes:

- *Monitoreo de noticias.*
- *Notificación de a sus superiores de posibles ataques cibernéticos, vulnerabilidades de equipos, plataformas u otros similares para evitar repercusiones en la institución*
- *Realizar recomendaciones para mitigación de daños en relación a reportes realizados.*

Responsabilidad de Trabajo # 6 — 5%

Encargado de coordinar capacitaciones de seguridad de la información: a empleados de la Institución

Tareas Permanentes:

- *Crear la información y presentaciones para capacitaciones sobre seguridad de la información para todos los empleados de la institución*
- *Capacitar al personal de la Gerencia de Informática en manejo de la seguridad de la información.*
- *Coordinar las capacitaciones con el Gerente y Jefes de Áreas.*
- *Documentar la realización de las capacitaciones y posibles mejoras para capacitaciones futuras.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 3 de resolución de Problema: Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. La persona debe ser analítico, crítico, investigativo y generador ideas, recomendaciones o soluciones a los problemas identificados.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☒ PRINCIPAL (asume completa y total responsabilidad)

☐ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Maestría o Post-grado en Administración de Redes o Computación, Seguridad Informática o áreas afines, capacitación en seguridad aplicada a sistemas de información, certificaciones o estudios en ISO 27001, COBIT, ISAE3402, SOX o ISO9000.
Educación Superior	☒	☐	Profesional Graduado en Ingeniería o , Licenciado en Sistemas Informáticos, o equivalente de educación

Experiencia

Indique la experiencia necesaria para el buen desempeño del puesto. Anote el número de años de experiencia profesional previa en una posición similar.

Requerida:

- Experiencia mínima de 5 años como Jefe en Seguridad de Informática o en puestos similares.

Deseable:

- Project Management
- Experiencia en arquitectura e implementación de proyectos de seguridad de la totalidad de los departamentos de IT.
- Conocimientos de auditoría
- Conocimientos en infraestructuras web,cloud computing y virtualización

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

	GERENCIAS, JEFES UNIDADES ASESORAS, JEFES DEPTO *(este grupo de comportamientos incluye al personal que desempeñan puestos con carácter de Gerencia y Jefaturas de Unidades Asesoras o Departamentos).*
A	**APTITUDES PERSONALES:** Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.
	Comportamientos evaluados:
	1. Conoce las funciones de su puesto?
	2. Demuestra dominio de conocimientos técnicos y especializados?
	3. Es hábil para buscar alternativas de solución?
	4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
	5. En momentos de crisis los problemas los resuelve con habilidad?
	CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.
	6. Es experto en los conocimientos concernientes a su área de trabajo, y permanentemente se actualiza en estos y en otros temas de interés que contribuyan a alcanzar los objetivos institucionales?
	7. Aplica los conceptos teóricos modernos y las mejores prácticas al desarrollo de sus actividades?
	8. Realiza propuestas de mejoramiento y está abierto a valorar las propuestas de otros para optimizar el desempeño?
	9. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios?
	10. Posee capacidad para resolver situaciones a corto y largo plazo?
	ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incremento de eficiencia en el personal.
	11. Es puntual en sus compromisos de trabajo?
	12. Organiza y programa adecuadamente su trabajo?
	13. Mantiene una actitud receptiva hacia la información o puntos de vista de otras personas?
	14. Inspira y transmite confianza en sus relaciones interpersonales?
	15. Es respetuoso y considerado con sus colaboradores?
	ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).
	16. Planifica sus acciones y las de su equipo de trabajo , considerando las necesidades de sus clientes (internos y/o externos)?
	17. Mantiene una comunicación efectiva con el cliente (interno y/o externo) para conocer sus necesidades y su nivel de satisfacción.
	18. Logra que los clientes (internos y/o externos) sientan que son lo más importante para la institución, manteniendo excelentes
	19. Actua como referente interno y/o externo cuando se busca aportar soluciones o satisfacer necesidades de sus clientes?
	20. Trabaja con una perspectiva de largo plazo a la hora de resolver los problemas del cliente (interno y/o externo), considerando sus impactos?
	LIDERAZGO : Entendido como la habilidad necesaria para orientar la acción de equipo de trabajo en una acción determinada, inspirando los valores en acción y anticipando escenarios de desarrollo de su equipo de trabajo.
	21. Lidera adecuadamente las reuniones (define agenda, establece fechas, los objetivos a discutir, controla el tiempo y asigna turnos de palabra, etc.)?
	22. Fija objetivos, los transmite claramente, realiza el seguimiento y brinda coaching sobre avances?
	23. Escucha y promueve la participación y la aportación de ideas?
	24. Delega y empodera a su equipo transmitiendo confianza y realizando un seguimiento efectivo?
	25. Tiene carisma propio, comunica una visión de futuro que genera entusiasmo y compromiso con la misión de la institución?

Habilidades Técnicas **Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:**

Requerida:

- Experiencia en seguridad de Redes, Firewall, proxy, filtrado de conexiones, análisis de paquetes, detección de ataques, etc.
- Experiencia en Seguridad de Sistemas operativos (windows server/linux/unix).Conocimientos de Seguridad Física y aspectos legales
- Conocimientos de antivirus, malware, adware, spyware, riskware, etc.
- Conocimientos de ataques web, SQL injection,XSS, XAS, CSRF, LFI/RFI, etc.
- Conocimientos de criptología: Encriptación, Cifrado simétrico/asimétrico, Clave pública, Clave privada, etc.

Deseable:

- Capacidad para evaluar las especificaciones técnicas y funcionales dentro del proceso de desarrollo de software, identificar las posibles amenazas o áreas de debilidad.
- Amplio conocimiento de la solicitud y las vulnerabilidades a nivel de infraestructura. Capacidad de explicar estos riesgos a los desarrolladores.

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes**	Para adquisiciones de productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

Condiciones de Trabajo

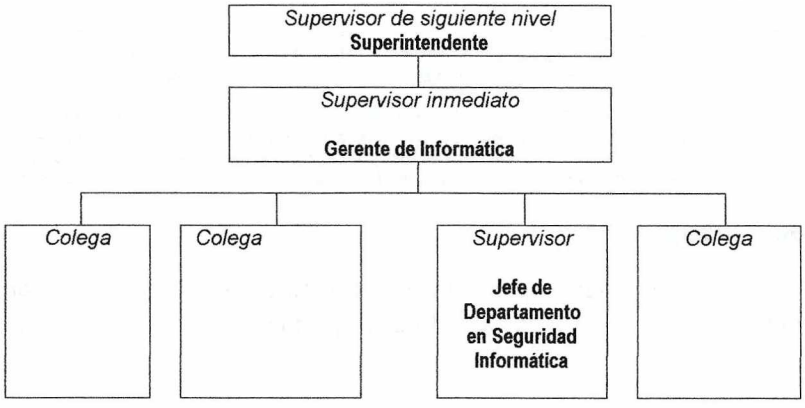
Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina **98%**

Porcentaje esperado de tiempo en viajes (al interior y exterior del país) **2%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



SECCIÓN 04

02

TÉCNICO EN SEGURIDAD INFORMÁTICA

Título del Puesto

GERENCIA DE INFORMÁTICA

Gerencia /Unidad Asesora/Jefatura Técnica

-11-
GRADO/NIVEL PUESTO

EXPERTO	**-1-**	**AGOSTO 2017**
Familia de Puesto	*Número de plazas*	*Fecha de Revisión de DP*

Objetivo del Puesto:

*En un párrafo breve, describa el propósito u objetivo general del puesto, haciendo énfasis en las funciones generales por las que la posición es responsable. **Por qué** existe el puesto y **qué debe lograr**, recuerde que NO se requiere una lista de actividades, sino la **Misión principal del puesto**.*

Implementar y dar seguimiento a la metodología de seguridad de la información de la institución y monitoreo de la seguridad de la red.

Responsabilidades:

Redacte un párrafo en donde describa las principales responsabilidades, tareas, capacidades y resultados por los que la posición es responsable (se recomienda limitar a ocho las responsabilidades). Incluya POR QUÉ es llevada a cabo y su impacto en la institución. Liste las responsabilidades en orden de importancia y mencione el porcentaje de tiempo que la persona utiliza en cada responsabilidad durante un año estándar.

Las personas que supervisan a otros, continuamente deben tener Supervisión de Personal como su Responsabilidad de Trabajo número uno. En donde, Supervisión total incluye: manejo de desempeño, contratación, despido, desarrollo y acompañamiento en el curso de sus actividades y deberes. La regla general para porcentajes de tiempo para la supervisión de otros es 5% por cada empleado-a de reporte directo. Ejemplo: si un supervisor-a tiene seis reportes directos, entonces por lo menos 30% de su trabajo deberá ser distribuido en la supervisión de estos empleados-as.

Responsabilidad de Trabajo # 1 — 30%

Apoyar en las gestiones de la seguridad aplicando metodologías, tecnologías y herramientas para las diversas áreas de la Institución en conjunto con el Jefe de Departamento en Seguridad de la Información.

Tareas Permanentes:

- *Apoyar en la implementación de políticas mediante configuraciones o instalaciones necesarias para el cumplimiento de procedimientos de seguridad.*
- *Realización periódica de los procedimientos de seguridad establecidos.*
- *Verificación y resolución de incidentes.*
- *Implementar herramientas y otras que fuera necesarias para la verificación de redes, sistemas operativos aplicaciones.*
- *Documentar todos los incidentes con recomendación para su manejo futuro.*

Responsabilidad de Trabajo # 2 — 25%

Ejecutar las rutinas de seguridad y las guías de implementación establecidas por el Jefe en Seguridad de la Información de la Institución.

Tareas Permanentes:

- *Desarrollar periódicamente tareas de pentest (penetration testing) y todo tipo de ataque ético (Ethical Hacking) con el fin de identificar y medir vulnerabilidades.*
- *Realizar un reporte de vulnerabilidades de todas las pruebas realizadas con sus recomendaciones de manejo.*
- *Conocer el plan de Disaster Recovery (estrategia de recuperación ante desastres) y los pasos para su ejecución.*
- *Realizar análisis de riesgos en nuevas tecnologías que se tengan en la institución.*
- *Asistir a los desarrolladores en la solución de vulnerabilidades.*
- *Responder a incidentes de seguridad física según indique su superior.*
- *Realizar actividades de gestión de riesgos (mitigaciones, capacitaciones entre otros).*

Responsabilidad de Trabajo # 3 — 25%

Monitorear noticias y medios relacionados a Seguridad de la Información en cuanto a temas relacionados a parches y actualizaciones de software de antivirus u otros similares para evitar repercusiones en la Institución.

Tareas Permanentes:

- *Monitoreo de noticias.*
- *Notificación a sus superiores de posibles* vulnerabilidades.
- *Notificar e implementar recomendaciones para mitigación de daños en relación a reportes realizados.*

Responsabilidad de Trabajo # 4 — 20%

Realizar capacitaciones de seguridad de la información a empleados de la Institución.

Tareas Permanentes:

- *Coordinar los recursos necesarios para la realización de capacitaciones.*
- *Brindar las capacitaciones a las áreas que están programadas.*
- *Documentar la realización de las capacitaciones y posibles mejoras para capacitaciones futuras.*

Resolución de Problemas

Es el proceso mental utilizado para resolver un problema (repetitivo o similar, complejo, no recurrente). El desafío del proceso aumenta cuando las variables cambian constantemente. Hay tres niveles de resolución de problemas:

1. Lo que hay que hacer y cómo hay que hacerlo están claramente definidos, y la persona enfrentará problemas **idénticos o similares regularmente;**
2. Lo que hay que hacer **es conocido**, pero cómo hacerlo no está definido. La persona ocupante de la plaza debe usar habilidades de análisis, reflexión interpretativa, evaluativa y/o constructiva.
3. Porqué se hacen las cosas es conocido, pero lo que se debe hacer y cómo debe hacerse no está definido. Las situaciones son variables, y la respuesta del titular involucrará análisis, definición del problema, desarrollo de alternativas, y hacer recomendaciones. Él o ella se enfrentará y resolverá problemas que son **típicamente no repetitivos**.

Por favor indique cuál de los niveles de solución de problemas descritos arriba enfrentará esta posición, y PORQUE la posición cabe en esa categoría.

La plaza se encuentra en un nivel 2 de resolución de Problema: Porqué lo que hay que hacer es conocido, pero como hacerlo no está definido. La persona debe de usar habilidades de interpolación para escoger la estrategia correcta para tratar el problema dado.

Libertad para Actuar / Impacto.

El grado en que las actividades del cargo **afectan y/o influyen directa o** indirectamente al logro de los **resultados esperados de la unidad.** Por favor seleccione el nivel de responsabilidad/contribución:

☐ PRINCIPAL (asume completa y total responsabilidad)

☒ CONTRIBUYE (provee apoyo y contribuye al éxito general)

☐ AUXILIAR (provee apoyo, pero contribuye indirectamente al éxito general)

Conocimientos y Capacidades *(Conocimiento Práctico)*

Indique el nivel mínimo requerido de educación, experiencia y habilidades necesarias para calificar a la posición y cumplir las expectativas de desempeño de trabajo que tenga la organización. Adicionalmente, incluya la educación, experiencia y habilidades deseables para la posición.

Educación

Ej.: Diploma de Bachillerato; diploma universitario (especificar grado y especialización o maestría); especialización (Contador Público Certificado, etc.). Incluya la siguiente frase cuando sea posible: "o combinación equivalente de educación y experiencia laboral"

Nivel de Enseñanza	Requerida	Deseable	Titulo Requerido
Post-grado (Especialización, Maestría, PhD)	☐	☒	Graduado en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación.
Educación Superior	☒	☐	Cursando Tercer año en Ingeniería o, Licenciatura en Sistemas Informáticos, o equivalente de educación; Técnico con certificaciones en seguridad o diplomados en seguridad de la información, certificaciones o estudios en ISO 27001, COBIT, ISAE3402, SOX o ISO9000.

Requerida:

- Experiencia mínima de 3 años como Técnico en Seguridad de Informática, o en puestos similares.

Deseable:

- Experiencia en seguridad de Redes, Firewall, proxy, filtrado de conexiones, análisis de paquetes, detección de ataques, etc.
- Conocimientos de Seguridad Física y aspectos legales
- Conocimientos de auditoría.

Habilidades Técnicas

Ejemplos: Idiomas, planificación, elaboración de presupuestos, procesamiento de datos, contaduría básica, comunicaciones escritas avanzadas, presentaciones, entrenamiento/facilitación, etc.:

Requerida:

- Experiencia en Seguridad de Sistemas operativos (windows server/linux/unix).
- Conocimientos de antivirus, malware, adware, spyware, riskware, etc.
- Conocimientos de ataques web, SQL injection,XSS, XAS, CSRF, LFI/RFI, etc.
- Conocimientos de criptología: Encriptación, Cifrado simétrico/asimétrico, Clave pública, Clave privada, etc.
- Ingles a nivel intermedio.

Deseable:

- Amplio conocimiento de la solicitud y las vulnerabilidades a nivel de infraestructura.
- Capacidad de explicar estos riesgos a los desarrolladores.

Competencias. **En función del nivel de responsabilidades del puesto, a continuación se enlistan las competencias y sus comportamientos asociados a la Familia de Puestos a la cual pertenece esta posición, los cuales son evaluados en el Proceso de Evaluación del Desempeño; pero en adición se espera que toda persona contratada modele dichos comportamientos en el día a día en su desempeño laboral. Favor leer detenidamente la información.**

B	**PERSONAL TECNICO Y ADMINISTRATIVO** *(este grupo incluye al personal que desarrollan labores técnicas y/o Administrativas en áreas especializadas de la institución).*
	APTITUDES PERSONALES: Conjunto de conocimientos básicos, técnicos y especializados de la competencias que permiten poner en práctica las habilidades necesarias , para el desempeño de las labores, de acuerdo a la naturaleza del puesto de trabajo.
	Comportamientos evaluados:
	1. Conoce las funciones de su puesto?
	2. Demuestra dominio de conocimientos técnicos y especializados?
	3. Posee capacidad propósitiva y criterio propio para solucionar las dificultades con sensatez y acudir en forma independiente y eficaz, sin necesidad de que se le proporcionen instrucciones?
	4. Posee habilidades para aplicar conocimientos teóricos y prácticos en la resolución de problemas de trabajo diario?
	5. Proporciona respuestas oportunas a las exigencias de trabajo?
	CALIDAD DE TRABAJO: Implica tener amplios conocimientos de los temas del área que éste bajo su responsabilidad, asi como también poseer la capacidad de comprender la esencia de los aspectos complejos, asegurando la eficacia y calidad de los resultados esperados en función de los objetivos institucionales.
	6. Identifica las tareas esenciales a realizar en el trabajo?
	7. Se dedica a cumplir con su trabajo en el plazo establecido, evitando distraerse con asuntos personales?
	8. La jornada laboral la realiza de manera responsable, lo cual le permite alcanzar resultados satisfactorios al finalizarla?
	9. Comprende la interrelación existente de trabajo entre su área y otras areas de la institución?.
	10. Frecuentemente realiza un esfuerzo mas allá de lo normal, para dar por finalizada una tarea asignada o problemas especificos?
	ACTITUDES PERSONALES: Conjunto de cualidades que rigen el comportamiento personal a efecto de fomentar principios y valores en el quehacer laboral y contribuir al incrmento de eficiencia en el personal.
	11. Es puntual en sus compromisos de trabajo?
	12. Organiza y programa adecuadamente su trabajo?
	13. Sabe como trabajar formando parte de un equipo?
	14. Inspira y transmite confianza en sus relaciones interpersonales?
	15. Es respetuoso y considerado con sus superiores y compañeros de trabajo?
	ORIENTACION AL CLIENTE INTERNO Y EXTERNO: Implica el compromiso por comprender y atender con calidad y transparencia los requerimientos de nuestros clientes externos (usuarios y operadores); asi como garantizar niveles de satisfacción en la entrega de los servicios a nuestros clientes internos (areas internas de la SIGET).
	16. Entiende con facilidad los problemas y/o necesidades de sus clientes (internos y/o externos)?
	17. Desarrolla soluciones a los problemas de los clientes (internos y/o externos), trabajando junto con ellos?
	18. Asesora y da al cliente (interno y/o externo) las alternativas que mejor se adaptan a sus necesidades?
	19. Se apega a los tiempos estipulados para la entrega de los servicios solicitados por los clientes (internos y/o externos), exigiéndose cumplir en tiempo y calidad?
	20. Hace más de lo que normalmente el cliente (nterno y/o externo) espera?

Contactos/Relaciones Clave

Liste las principales relaciones internas y externas, las cuales se espera el empleado mantenga. Detalle brevemente el propósito de estas interacciones (incluyendo cualquier implicación significativa en comités).

	Área/Organización	Propósito de la Relación
Internos	**Todas las Unidades y Gerencias de la Organización**	Gestionar solicitudes e intercambio de información.
Externos	**Proveedores de servicios y bienes**	Adquirir productos como licencias, sistemas, servicios de internet, servicios de mantenimiento y capacitación.

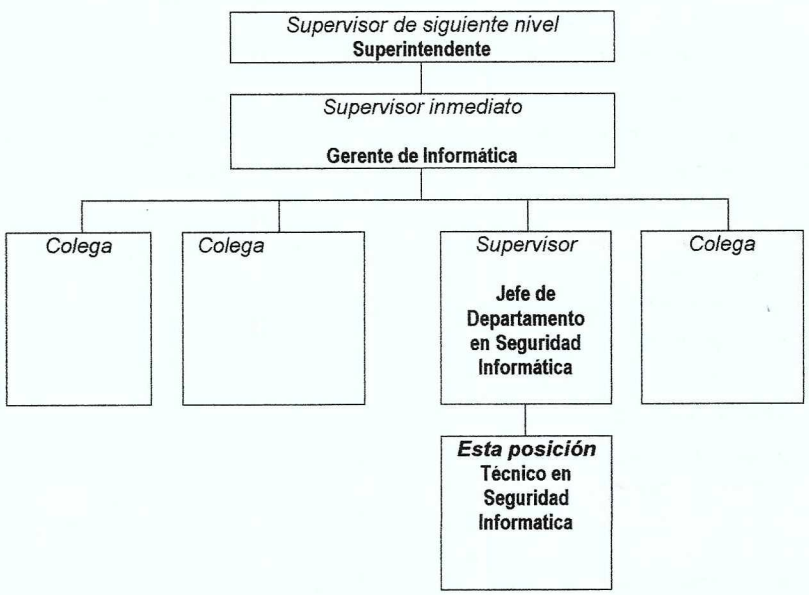
Condiciones de Trabajo

Escriba la locación de trabajo, el porcentaje de viaje esperado, y condiciones especiales que apliquen para la posición.

Trabajo Administrativo/Oficina	**98%**
Porcentaje esperado de tiempo en viajes (al interior y exterior del país)	**2%**

Organización

Coloque en la casilla remarcada el nombre del cargo del ocupante de la plaza, en las casillas superiores el cargo al cual le reporta, en las casillas inferiores los nombres de los cargos que le reportan al ocupante de la plaza y en los paréntesis (horizontal) a la derecha e izquierda algunas posiciones que serán sus colegas.



CAPITULO VI LISTADO DE DISTRIBUCION, REVISIONES Y EDICIONES

SECCIÓN 00 SECCION UNICA

1) Edición:

Fecha	Persona	CC	Area	Recibido

2) Distribución Adicional:

Fecha	Documento Revisado	C.C.	Persona	Recibido

3) Revisiones (Modificaciones por Capítulo):

Fecha	Revisión N°	Capítulo Afectado	Página Modificada	Autorizado

4) Listado de Ediciones / Histórico:

Fecha	Observaciones