Resolución de Gerencia N° 065-2020-MDB/GM

Bellavista, 29 de diciembre de 2020

EL GERENTE MUNICIPAL DE LA MUNICIPALIDAD DISTRITAL DE BELLAVISTA

VISTO:

El Informe N° 094-2020-MDB-GM/SGTIC de la Sub Gerencia de Tecnología de la Información y Comunicaciones;

CONSIDERANDO:

Que, el primer párrafo del artículo 194 de la Constitución Política del Perú, precisa que las Municipalidades son órganos de Gobierno Local y tienen autonomía política, económica y administrativa en los asuntos de su competencia. Asimismo, el artículo II del Título Preliminar de la Ley N° 27972 – Ley Orgánica de Municipalidades, al referirse a la autonomía de los Gobiernos Locales, precisa que ésta emana de la Constitución y radica en la facultad de ejercer actos de gobierno, administrativos y de administración, con sujeción al ordenamiento jurídico.

Que, mediante Resolución Ministerial N° 246-2007-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición", en todas las Entidades integrantes del Sistema Nacional de Informática.

Que, mediante Resolución Ministerial N° 004-2016-PCM se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

Que, el Reglamento de Organización y Funciones de la Municipalidad Distrital de Bellavista, aprobado mediante Ordenanza Municipal N° 011-2017-CDB, establece en su artículo 62 que la Sub Gerencia de Tecnología de la Información tiene entre sus funciones: administrar el sistema de red local, velando por un adecuado uso, tanto del hardware como del software a fin de lograr su óptimo rendimiento; formular y supervisar la aplicación de los planes de contingencias y de seguridad de la información que aseguren la continuidad de la gestión de la Municipalidad, para la implementación de los planes mencionados; formular, elaborar y ejecutar el plan de contingencia informático y de comunicaciones, a fin de garantizar la normal operatividad de la red, los servicios de internet, correo electrónico y transmisión de datos.

Que, bajo este marco normativo, mediante Informe N° 094-2020-MDB-GM/SGTIC del 24 de noviembre de 2020, la Sub Gerencia de Tecnología de la Información y Comunicaciones presenta para su aprobación un proyecto de Plan de Contingencias de Tecnología de Información y Comunicaciones, el cual también contiene doce formatos para el registro de información, que servirán como base para la elaboración del Plan de Gobierno Digital y para el proyecto de Gobierno Digital que la mencionada Sub Gerencia tiene previsto elaborar en el año 2021.

Que, la elaboración y aprobación del presente Plan de Contingencia, se enmarca también dentro del proceso de implementación de la recomendación N° 6 del Informe de Auditoría de Cumplimiento N° 010-2016-2-1619, "Adquisición al Sistema de Gestión Tributaria", que propone el inicio de la implementación de las Normas Técnicas Peruanas que son de uso obligatorio para todas las entidades del Estado.

Que, mediante Resolución de Alcaldía Nº 553-2019-MDB/AL del 4 de setiembre de 2019 se delegó en el Gerente Municipal la facultad de aprobar directivas y documentos de carácter normativo necesarios para conducir la gestión técnica, financiera y administrativa de la Municipalidad;

Estando a lo expuesto, con el visto bueno de la Gerencia de Asesoría Jurídica y de la Sub Gerencia de Tecnología de la Información y Comunicaciones; y, de conformidad con las atribuciones delegadas a la Gerencia Municipal mediante Resolución de Alcaldía Nº 553-2019-MDB/AL;

RESUELVE:

ARTÍCULO PRIMERO.- Aprobar el **PLAN DE CONTINGENCIAS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES,** cuyo texto y formatos adjuntos, forman parte integrante de la presente Resolución.

ARTÍCULO SEGUNDO.- Encargar a la Sub Gerencia de Tecnología de la Comunicación y Comunicaciones el cumplimiento de lo dispuesto en la presente Resolución.

ARTÍCULO TERCERO.- Encargar a la Sub Gerencia de Tecnología de la Información y Comunicaciones la publicación de la presente Resolución en el Portal Institucional www.munibellavista.gob.pe y en el Portal de Transparencia Estándar de la Municipalidad Distrital de Bellavista.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE

MUNICIPALIDAD DISTRITAL DE BELLAVISTA
CESAR AUGUSTO AGUILAR VILLEGAS
Gerente Municipal

MUNICIPALIDAD DISTRITAL DE BELLAVISTA

BELLAVISTA confía en ti

PLAN DE CONTINGENCIAS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Bellavista, 2020

MUNICIPALIDAD DISTRITAL DE BELLAVISTA
V°B°

INTRODUCCIÓN

El Plan de Contingencia de Tecnologías de Información y Comunicaciones de la Municipalidad distrital de Bellavista, es un documento que establece la planificación de procedimientos de respuestas estratégicas de emergencia para:

- Reducir a niveles aceptables la interrupción causada por desastres y fallas de seguridad, mediante una combinación de controles preventivos y de recuperación.
- Identificar los procesos críticos e integrar los requisitos de gestión de seguridad de información para la continuidad de las actividades de la Municipalidad.

1. GENERALIDADES

1.1 Definición del Plan de Contingencia

Un plan de contingencias es una estrategia planificada, con una serie de procedimientos que nos facilitan o nos orientan, a tener una solución alternativa para restituir rápidamente los servicios de la organización, ante eventos que puedan paralizarlos de forma parcial o total.

1.2 Objetivos del Plan de Contingencia

Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información para la Municipalidad.

Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información.

1.3 Objetivos Específicos

- Proteger la vida de las personas inherentes a los servicios informáticos de la Municipalidad.
- Prevenir o minimizar la pérdida o la corrupción de archivos de datos criticos para la continuidad de las operaciones de la Municipalidad.
- Proteger la propiedad de la Municipalidad y otros activos.
- Iniciar un procedimiento de recuperación de los servicios informáticos ante un desastre o falla.
- Continuar con las funciones de las diferentes Unidades Orgánicas de la Municipalidad que se hayan visto afectadas por una situación adversa.

- Prevenir o minimizar el daño permanente a los recursos informáticos.
- Minimizar el número de decisiones a tomar ante la presentación de un desastre.
- Minimizar las dependencias específicas durante el proceso de recuperación.
- Minimizar la necesidad de probar acciones de recuperación corriendo el riesgo de cometer errores cuando ocurra una emergencia o desastre.

1.4 Base Legal

- Resolución Ministerial N Q 246-2007-PCM que dispone el uso obligatorio de la Norma Técnica Peruana - ISO/IEC 17799:2007 EDI. Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información".
- Reglamento de Organización y Funciones, aprobado con Ordenanza N° 011-2017-CBD del 25 Julio 2017.

1.5 Responsabilidad de la elaboración.

De acuerdo a la sección IV, articulo 62, inciso I) del Reglamento de Organización y Funciones (ROF) aprobada con Ordenanza N° 11-2017-CBD, es responsabilidad de la Sub Gerencia de Tecnologías de Información y Comunicación (GTIC) "Formular y supervisar la aplicación de los planes de contingencias y de seguridad de la información que aseguren la continuidad de la gestión de la Municipalidad, para la implementación de los planes mencionados."

1.6 Actualización del Plan de Contingencia

Este Plan de Contingencia será revisado y actualizado de manera periódica una vez por año.

A continuación, se indica la responsabilidad y el proceso de actualización:

1. Sub Gerente de Tecnologías de Información y Comunicación ordena actualización del Plan de Contingencia.
2. Equipo Desarrollo de Sistemas y Equipo de Plataforma Tecnológica elaboran o actualizan el Plan de Contingencia ante cambios en el entorno de los procesos, operaciones críticas y recursos/servicios en la Municipalidad.

3. Sub Gerente de Tecnologías de Información y Comunicación da V.B. a actualización del Plan de Contingencia y solicita aprobación coordinando con la Gerencia Municipal.

1.7 Publicación y Difusión

La SGTIC publicará un documento impreso del Plan de Contingencia, el mismo que mantendrá al alcance del personal del área, en un lugar de acceso y conocimiento del personal, para su difusión y correcta utilización en caso sea necesario.

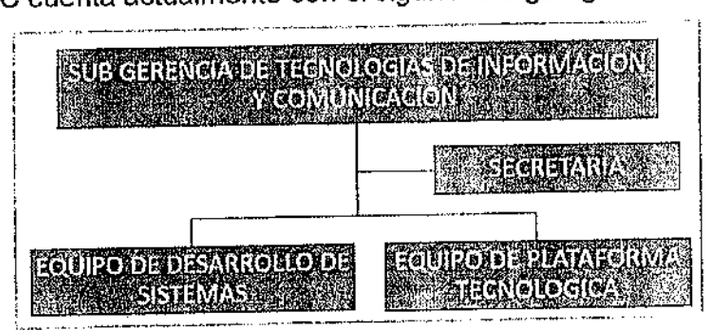
Se publicará una versión resumida (sin anexos) en el portal Web de la Institución, por considerarse información de carácter reservada, previa Resolución Gerencial.

1.8 Alcance

Este Plan de Contingencia es de aplicación para los equipos informáticos y de comunicación de usos internos o externos, propios o rentados, de la Municipalidad y que se encuentren bajo la responsabilidad de la Sub Gerencia de Tecnologías de Información y Comunicación.

II. SITUACIÓN ACTUAL DE LOS RECURSOS INFORMÁTICOS Y ORGANIZACIÓN DE LA SGTIC

La SGTIC cuenta actualmente con el siguiente organigrama funcional (interno)



- Sub Gerente de Tecnologías de Información y Comunicación (SGTIC), funcionario de confianza encargado de la SGTIC.
- Secretaría y Auxiliar de Sistema Administrativo, encargado de la entrada y salida de documentación del área.
- Equipo de Desarrollo de Sistemas: Personal Técnico encargado del desarrollo de nuevas aplicaciones y mantenimiento de las aplicaciones existentes de la Municipalidad.
- Equipo de Plataforma Tecnológica: Personal Técnico encargado de soporte técnico, red de comunicaciones, servidores, cámaras de video vigilancia

EQUIPO PLATAFORMA DE TIC

Para una adecuada respuesta ante cualquier eventualidad o falla ocurrida a cualquier recurso informático físico de la Municipalidad, se tiene el inventario completo de todos los elementos y sus respectivas ubicaciones. Este inventario está compuesto por:

a) Computadoras de Escritorio y Portátil de propiedad de la Municipalidad.

El inventario de las estaciones de trabajo o computadoras destinadas al uso del personal de la municipalidad, así como los equipos portátiles, se encuentra en el anexo 01 correspondiente.

b) Periféricos

El inventario de periféricos de la Municipalidad, tales como: Scanner, Impresoras (Inyección, Matricial, Láser, Térmica), Fotocopiadoras, Monitores, anexos, se encuentra descrito en el anexo 02 correspondiente.

c) Equipos Cámaras y de Videos CCTV

El inventario de cámaras internas de la Municipalidad se encuentra descritos en el anexo 03 correspondiente.

MUNICIPALIDAD DISTRITAL DE ELLAVISTA
V°B°

d) Red de área Local corporativa.

La Municipalidad cuenta con 11 locales, de los cuales 09 se encuentran interconectados mediante enlaces Inalámbricos y 02 locales no están interconectados.

Sedes Municipales			
Ítem	**Sede**	**Dirección**	**Observación**
1	PALACIO MUNICIPAL	Jr. francisco Bolognesi 498, Bellavista.	Interconectado
2	CASA DE LA JUVENTUD	Jr. Los Heros 2, cruce con Comandante Espinar	Interconectado
3	OMAPED - OPV	Calle More Mz. E Lt. 6, Urb. Proción	Interconectado
4	SUB GERENCIA DE SERENAZGO	Parque Pescadito	Interconectado
5	CIS	Eucaliptos s/n. Av. Venezuela con Av. Elmer Fauccet	Interconectado
6	SANIDAD	Parque Pescadito	Interconectado
7	PIO XII	Jr Grau 495	Interconectado
8	SERVICIOS A LA CIUDAD - MAESTRANZA	Av. Prolongación Buenos Aires 2176	Interconectado
9	MALL	Centro Comercial del MALL PLAZA. 1er piso Tottus	No interconectado. Cuentan con servicio de internet propio con la empresa

			Claro. Hay 2 usuarios
10	ESTADIO GUALBERTO LIZARRAGA	Calle 7, Ciudad Pescador	Interconectado
11	LOCAL DE SANIDAD – SAN JOSE	Calle Atillio Batifora N° 140 (Frente al Parque Daniel Woll)	No interconectado. Hay tres PCs, cuentan con internet que la dueña del local provee.

e) Equipos de Comunicaciones Voz y Data.

El inventario de los equipos; que son utilizados para las comunicaciones de Voz y Data entre los 09 Locales de la municipalidad interconectados, tales como Switches, Central telefónica, radios de comunicación inalámbrica, antenas, etc.; se encuentra en el anexo 04 correspondiente.

Se aprecia una variedad de marcas y fabricantes en los Equipos de Comunicación que posee la municipalidad, lo que implica contar con profesionales y técnicos especializados, a fin de prever, analizar, diagnosticar y solucionar las diferentes dificultades que se presenten y/o efectuar la coordinación de la solución de los problemas con los proveedores de cada marca y/o fabricante.

f) Equipos Servidores.

El inventario de servidores que soportan la operatividad de todos los Sistemas de Información de la municipalidad se encuentra en el anexo 05 correspondiente.

La municipalidad cuenta con servidores físicos para soportar todos los sistemas informáticos, se cuenta adicionalmente con equipamiento tecnológico para la seguridad perimetral como Firewall.

SERVICIOS Y SISTEMAS DE INFORMACIÓN

a) Responsables de los Sistemas de Información.

Los sistemas de Información están bajo responsabilidad de las áreas usuarias y son responsables de emitir las Órdenes de Trabajo para mantener y/o mejorar estos sistemas.

El mantenimiento y actualización de los Sistemas Informáticos de propiedad de la municipalidad está a cargo de la Sub Gerencia de Tecnologías de Información y Comunicaciones.

Las características generales de cada sistema de Información y de los responsables del mantenimiento se encuentra en el anexo 06 correspondiente.

b) Licencias de Software

La Sub Gerencia de Tecnologías de la Información y Comunicación administra las licencias recursos de Software se encuentra en el anexo 07 correspondiente.

c) Bases de Datos

La Sub Gerencia de Tecnologías de la Información y Comunicación administra las bases de datos de producción y de desarrollo. Las bases de datos con la que se cuenta se encuentran en el anexo 06 correspondiente.

d) Servicios de Internet.

El servicio de internet de 50 MBPS que cuenta la municipalidad es brindado por la empresa GTD Wigo. Se cuenta con redundancia del servicio.

Contacto: Ramos, Fernando fernando.ramos@grupogtd.com

Soporte: https://www.gtdperu.com/soporte

e) Dominios y subdominios publicados en Internet.

Sitio web: www.punto.pe

Los datos de contacto para la actualización de los dominios están configurados con la cuenta: mauro.valencia@munibellavista.gob.pe

La relación de dominios en Internet y su respectivo estado se encuentran en el anexo 08 correspondiente.

MUNICIPALIDAD DISTRITAL DE BELLAVISTA

f) Servicio de Correo electrónico

El Servicio de Correo se brinda es por medio de ZIMBRA, utilizando los dominios MUNIBELLAVISTA.GOB.PE. Los usuarios de correo electrónico acceden a este servicio, utilizando sus respectivas cuentas y claves, mediante la siguiente URL https://mail.munibellavista.gob.pe/

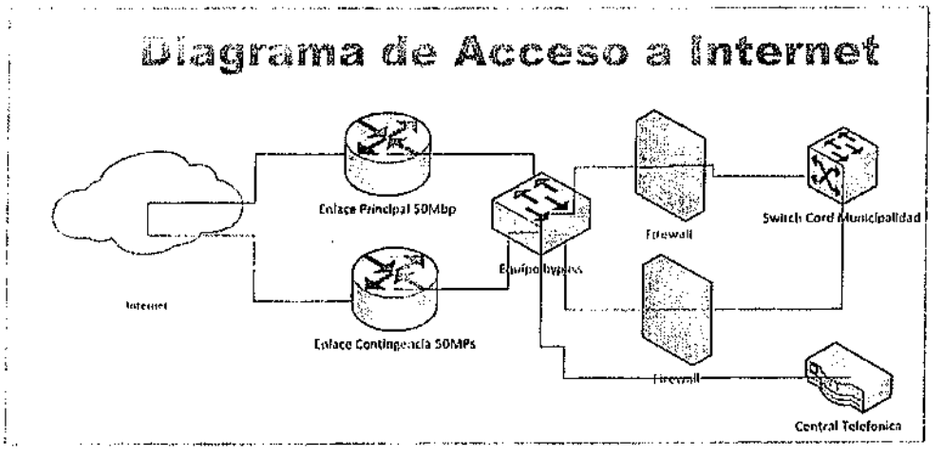
Todos los funcionarios, personal CAS y personal estable que han solicitado sus cuentas de correo, se encuentran empadronados con registros adecuados y supervisados.

h) Red Corporativa

El inventario consolidado de Equipos Informáticos que forman parte de la Red Informática de la Municipalidad, se muestra en el anexo 09 correspondiente.

Los equipos de cómputo y periféricos que forman parte de la Red Informática de la municipalidad, se encuentran configuradas bajo DOMINIO y cuenta con Seguridad Perimetral basada en un Firewall con equipo PALOALTO.

El Firewall actúa como barrera de contención a posibles ataques externos (de una red externa a la red interna de la Municipalidad) que puedan darse. Asimismo, se encarga de controlar los accesos de los usuarios de la municipalidad hacia Internet, restringiendo de acuerdo a los niveles y permisos inherentes de cada usuario. En el Firewall se encuentran las políticas de acceso, medición del ancho de banda, permisos, grupos, reglas que estén implementadas para la seguridad y acceso del servicio de internet.



La interconexión entre los locales administrativos de la municipalidad es 100% inalambrica.

MUNICIPALIDAD DISTRITAL DE BELLAVISTA
V°B°

i) Dominio

La Red Informática de la Municipalidad está configurada con Dominio Windows Server Standard 2016. Esta configuración facilita las tareas de administrar la red, ya que permite realizar una agrupación lógica de servidores de red y otros ordenadores, para compartir información común sobre cuentas y seguridad.

La Municipalidad cuenta con un Servidor de dominio Principal y un Secundario.

Por razones de Seguridad Informática y por Política de la Municipalidad, todos los equipos que conforman el Parque Informático de la Municipalidad, deben estar configurados con Dominio, sólo de esta manera puedan hacer uso de los Recursos Informáticos de la Municipalidad.

GESTIÓN DE INCIDENCIAS

La Gestión de Incidentes tiene como objetivo prever y resolver cualquier incidente que cause una interrupción en el servicio de la manera más eficiente y eficaz posible.

La información es inherente a las actividades que realiza la Municipalidad y su correcta gestión debe apoyarse en tres pilares fundamentales:

- **Confidencialidad**: la información debe ser sólo accesible a sus destinatarios predeterminados.
- **Integridad**: la información debe ser correcta y completa.
- **Disponibilidad**: debemos de tener acceso a la información cuando la necesitamos. La Gestión de la Seguridad Informática; implica velar por que la información sea correcta y completa, esté siempre a disposición de las actividades de la municipalidad y sea utilizada sólo por aquellos que tienen autorización para hacerlo.

a) Mantenimiento Preventivo y Correctivo.

Actúan sobre la vulnerabilidad de los activos y reducen la potencialidad de materialización de la amenaza. Son salvaguardas, la detección preventiva, la información y formación del personal. Para ver el detalle se debe ver ir al Procedimiento preventivo y correctivo de equipos de cómputo.

b) Acceso a sistemas informáticos

Para ver el detalle se debe ver ir al Procedimiento preventivo y correctivo de equipos de cómputo.

c) Acceso a recursos tecnológicos

Para ver el detalle se debe ver ir al Procedimiento preventivo y correctivo de equipos de cómputo.

d) Backup de Información.

La periodicidad de backup se detalla en el anexo 10 correspondiente.

e) Claves de los Servidores

Las claves de los Servidores de la Municipalidad se encuentran custodiadas por la Sub Gerencia de Tecnologías de Información y Comunicaciones.

PROTOCOLO PARA INCIDENTES INFORMÁTICOS

a) Situación: Ingreso no autorizado al portal institucional y servicios en línea y alteración del contenido.

Paso 1: Comunicarse con Procuraduría Publica Municipal, para que tenga conocimiento del hecho y pueda sentar la denuncia policial.

Paso 2: Se dará de baja el servicio web a fin que la página web no siga mostrando la información alterada a la espera de la presencia de un representante legal, para formalizar la denuncia.

Paso 3: Una vez realizada la visita del personal legal, se reemplazarán las contraseñas del servidor y servicios de consolas administrativas involucradas con el servidor web.

Paso 4: Una vez realizada el reemplazo de la contraseña, realizar un Backup de la página web con la información alterada para tener evidencias de lo ocurrido.

Paso 5: Realizado el Backup se procederá a corregir la información alterada en la página y se realizará el análisis forense correspondiente de lo ocurrido.

Paso 6: Elaborar un informe correspondiente de lo ocurrido incluyendo todas evidencias encontradas.

b) Situación: Envío de correo que agredan la integridad del personal.

Paso I: Comunicarse con Procuraduría Publica Municipal, para que tenga conocimiento del hecho y puede comunicarse con la DIVINDAT-DIRINCRI y/o Notaria a fin de sentar la denuncia policial.

Paso 2: El personal de la Sub Gerencia de Tecnologías de Información y Comunicaciones se apersonará para revisar el equipo de cómputo a donde llegaron los correos difamatorios.

Paso 3: El personal de la Sub Gerencia de Tecnologías de Información y Comunicaciones capturará toda la información relevante y sea conveniente para poder realizar el análisis forense correspondiente.

Paso 4: Elaborar un informe correspondiente de lo ocurrido incluyendo todas evidencias encontradas.

Paso 5: El personal de la Sub Gerencia de Tecnologías de Información y Comunicaciones de acuerdo a lo que se le solicite, bloqueará o no el correo remitente, para así evitar la recepción de más correos.

c) Situación: Publicación de páginas web ajenas a la Municipalidad que agredan la integridad del personal.

Paso 1: Comunicarse con la Procuraduría Publica Municipal, para que tenga conocimiento del hecho y pueda comunicarse con la DIVINDAT-DIRINCRI y/o notaria a fin de sentar la denuncia policial.

Paso 2: El personal de la Sub Gerencia de Tecnologías de Información y Comunicaciones realizará todos los trámites respectivos para poder sentar la denuncia y solicitar la baja respectiva de la página web.

Paso 3: El personal de la Sub Gerencia de Tecnologías de Información y Comunicaciones capturará toda la información relevante

Paso 4: Elaborar un informe respectivo de lo ocurrido incluyendo todas las evidencias encontradas

III. IDENTIFICACIÓN DE RIESGOS Y ESTRATEGIAS

3.1. ANÁLISIS DE RIESGO

En esta sección se definen las operaciones y/o servicios críticos que son brindados por la Sub Gerencia de Tecnologías de Información y Comunicaciones, y cuya operatividad debe ser recuperada rápidamente, de acuerdo a los procedimientos establecidos, de forma tal que se asegure la continuidad de los mismos. Aquí es importante especificar cuál es la prioridad de la operación, de forma tal que se pueda establecer una secuencia de recuperación en caso de desastre en varios de ellos.

a) Niveles de importancia en la selección de las operaciones: Operaciones críticas definidas en función a los componentes de los sistemas de información: Datos, Aplicaciones, Tecnología Hardware y Software, instalaciones y personal. Niveles: Alta (A), Media (M) y Baja (B)

Procesos críticos – Objetivos de operación – Grado de importancia		**A**	**M**	**B**
Servidores				
01	Servidor de Correo	X		
02	Servidor SIAF	X		
03	Servidor WEB Institucional		X	
04	Central Telefónica	X		
05	Servidor de Base de Datos	X		
06	Servicio de Internet	X		
07	Servidor de Dominio	X		
08	Servicio de Antivirus		X	
09	Servicio de red de datos	X		
10	Servicio de Cámaras internas	X		
11	Servicio de Fluido Eléctrico	X		
Sistemas de información		**A**	**M**	**B**
01	Sistema de Administración Tributaria	X		

02	Sistema de Trámite Documentario	X		
03	Portal Institucional		X	
04	Sistema de colas			X
05	SIGA	X		
06	MUNIBE_SIS (Modulo Intranet)			X
07	MUNIBE_SIS (Módulo Juntas Vecinales)			X
08	MUNIBE_SIS (Módulo Normas)	X		
09	MUNIBE_SIS (Módulo PIDE)		X	
10	MUNIBE_SIS (Módulo Vaso de Leche)	X		

b) Lista de periodos aceptables de interrupción

El siguiente cuadro muestra los periodos de interrupción aceptables para los servicios y/o recursos. Los planes de mitigación de riesgos y los planes de recuperación deberán tomar en cuenta estos periodos de recuperación a fin de que se ajusten a los mismos.

También es importante identificar el impacto que tendría cada recurso para tomar acción sobre ellos.

Periodos aceptables de recuperación/Impacto				
Nª	**Recurso**	**Posibilidad**	**Periodo necesario para la recuperación**	**Impacto**
01	Servidor de correo	MEDIO	12 HORAS	ALTO
02	Servidor SIAF	BAJO	4 HORAS	ALTO
03	Servidor WEB Institucional	BAJO	4 HORAS	MEDIO
04	Central Telefónica	BAJO	2 DIAS	ALTO
05	Servidor de Base de Datos	BAJO	4 HORAS	ALTO
06	Servicio de Internet	BAJO	2 HORAS	ALTO
07	Servidor de Dominio	BAJO	2 HORAS	ALTO
08	Servicio de Antivirus	BAJO	2 HORAS	MEDIO
09	Servicio de red de datos	BAJO	8 HORAS	ALTO
10	Servicio de Cámaras	BAJO	4 HORAS	ALTO
11	Estaciones de trabajo	MEDIO	3 HORAS	ALTO
12	Radio enlaces	BAJO	1 DIA	ALTO
11	Servicio de Fluido Eléctrico	MEDIO	4 HORAS	ALTO

MUNICIPALIDAD DISTRITAL DE BELLAVISTA V°B°

c) Lista de recursos utilizados

Se detallan los proveedores de los recursos en caso suceda incidencias

Recursos utilizados		
Nª	**Recurso**	**Proveedor**
01	Servidor de correo	SGTIC
02	Servidor SIAF	SGTIC – MEF
03	Servidor WEB Institucional	SGTIC
04	Central Telefónica	SGTIC - GTD
05	Servidor de Base de Datos	SGTIC
06	Servicio de Internet	GTD
07	Servidor de Dominio	SGTIC
08	Servicio de Antivirus	SGTIC – ITERA SAC
09	Servicio de red de datos	SGTIC
10	Servicio de Cámaras internas	SGTIC
11	Estaciones de trabajo	SGTIC – Ver garantía según compra.
12	Radio enlaces	SGTIC
13	Sistemas de información (Interno y externo)	Ver anexo correspondiente
14	Fluido Eléctrico	Sub Gerencia de Logística - ENEL

d) Especificación de escenarios

Se define como desastre a cualquier evento que puede interrumpir el normal funcionamiento de las operaciones y/o servicios especificados.

En ese contexto, a continuación, se detallan los posibles escenarios de "desastres' (fallas):

(i) SERVIDORES

- **Situación: Falla del servidor y/o dispositivo. (Hardware) Falla total o parcial del hardware del servidor.**

  Contingencia: Ejecución del procedimiento de configuración del servidor, según sea el caso. Ver el anexo correspondiente.

- **Situación: Falla de servicio (Software)**

  Daño del Sistema Operativo o alguno de sus componentes.

MUNICIPALIDAD DISTRITAL DE BELLAVISTA V°B°

Contingencia: Ejecución del procedimiento de instalación de servicios, según sea el caso. Ver el anexo correspondiente

- **Situación: Ataque de denegación de servicio en los diferentes servidores.**
  - Paso 1: Aislar Equipo
  - Paso 2: Revisión de los logs del sistema.
  - Paso 3: Revisión de los puertos abiertos del Servidor para la resolución de problemas / Utilización del Netstat)
  - Paso 4: Comunicarse son el proveedor de internet.
  - Paso 5: Identificar el ataque y tomar las acciones correctivas para cortarlo.
  - Paso 6: Restablecer la operatividad del Servicio.
- **Situación: Error de memoria en un servidor**
  - Paso 1: Avisar a los usuarios que deben salir del sistema.
  - Paso 2: Deshabilitar entrada al sistema para que usuarios no reintenten ingreso.
  - Paso 3: Bajar el sistema y apagar el equipo.
  - Paso 4: Retirar la memoria de computador y colocarla nuevamente.
  - Paso 5: Iniciar la máquina nuevamente y revisar el estado de la memoria.
  - Paso 6: En caso persista la falla con la memoria, reemplazarla por una memoria de las mismas características.
- **Situación: Error de tarjetas controladoras**
  - Paso 1: Avisar a los usuarios que deben salir del sistema.
  - Paso 2: El servidor debe estar apagado, dando un correcto apagado del sistema.
  - Paso 3: Ubicar la posición de la tarjeta controladora.
  - Paso 4: Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.
  - Paso 5: Retirar la conexión del Servidor con el Switch de red, está ubicada detrás del servidor, ello evitará que, al encender el sistema, los usuarios ingresen.

- Paso 6: Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar las entradas para estaciones de trabajo en las cuales se realizarán las pruebas.
- Paso 7: Habitar las entradas al sistema para los usuarios.

- **Situación: Error fisico del disco en un servidor**
  - Paso 1: Ubicar el disco malogrado
  - Paso 2: Avisar a los usuarios que deben salir del sistema.
  - Paso 3: Deshabilitar entrada al sistema para evitar que usuarios reintente ingreso.
  - Paso 4: Bajar el sistema y apagar el equipo.
  - Paso 5: Retirar el disco defectuoso.
  - Paso 6: Reemplazar el disco por uno de las mismas características que el sustraído y colocarlo dentro del Servidor.
  - Paso 7: Formatear el nuevo disco y darle partición.
  - Paso 8: Restaurar último backup en nuevo disco y verificar su estado, luego restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
  - Paso 9: Habilitar las entradas al sistema para los usuarios.

(ii) ESTACION DE TRABAJO

- **Situación: Error de memoria en una estación de trabajo**
  - Paso 1: Retirar la memoria de computador y colocarla nuevamente.
  - Paso 2: Iniciar la máquina nuevamente y revisar el estado de la memoria.
  - Paso 3: En caso persista la falla con la memoria, probarla en otra PC con las mismas características para ubicar la memoria defectuosa
  - Paso 4: Reemplazar por una memoria de las mismas características

- **Situación: Borrado involuntario de archivos**
  - Paso 1: Coordinar con el usuario que solo se asegura la recuperación a un 40 % de los archivos eliminados.
  - Paso 2: Instalar la herramienta de recuperación de archivos

- Paso 3: Indicar la ruta y el tipo de archivos borrados.

(iii) SISTEMAS DE INFORMACIÓN

- **Situación: Confinamiento de programa malicioso de una PC o Servidor**
  - Paso 1: Revisión de alguna carpeta compartida en el computador o Servidor.
  - Paso 2: Búsqueda por medio de un Software especializado de algún troyano que este robando los archivos.
  - Paso 3: Eliminación del programa.
  - Paso 4: Actualizar el Sistema Operativo en caso sea necesario.
- **Situación: Robo de información por intrusión en la base de datos**
  - Paso 1: Revisión de los accesos.
  - Paso 2: Revisión del log del Sistema
  - Paso 3: Anulación de la vulnerabilidad.
- **Situación: Robo de información por usurpación de identidad.**
  - Paso 1: Llamar al personal del Equipo de Desarrollo de Sistemas de Información
  - Paso 2: Cambio de Contraseña del Usuario Comprometido.

(iv) PORTAL MUNICIPAL

- **Situación: Falla en el Portal Institucional.**
  - Paso 1: Revisión de los servicios del servidor y Base de datos
  - Paso 2: Revisión general del Servidor

(v) CENTRAL TELEFONICA

- **Situación: Central telefónica - error de conectividad**
  - Paso 1: Revisión de los cables de la Central Telefónica.
  - Paso 2: Revisión que ningún usuario este utilizando el IP de la Central Telefónica.
  - Paso 3: En caso sea cualquiera de los dos problemas antes mencionados, revisar y proceder a realizar los cambios necesarios.

MUNICIPALIDAD DISTRITAL DE BELLAVISTA
V°B°

- **Situación: Central telefónica - Corte de energía eléctrica**
    - Paso 1: Revisión de los cables poder de la Central Telefónica
    - Paso 2: En caso se encontrase desconectada, volver a conectarla al fluido eléctrico y esperar que encienda normalmente.

(vi) SOFTWARE

- **Situación: Falla en el software**
    - Paso 1: Llamar al personal del Equipo Funcional de Plataforma Tecnológica
    - Paso 2: Revisar el software instalado y verificar si contiene errores
    - Paso 3: Según el listado de licencia de software revisar si corresponde la instalación del software, y de ser así instalarlo en la máquina usuaria.

(vii) LINEAS DEDICADAS

- **Situación: Falla de un de conectividad de red (WAN).**
    - Falla parcial o total del equipo de conectividad (Route)
    - Contingencia: Se cuenta con un equipo de similares características, el cual se encuentra disponible.
- **Situación: Falla de un equipo de conectividad de red (LAN).**
    - Falla parcial o total del equipo de conectividad (Switch)
    - Contingencia: Cambio de equipo de conectividad según disponibilidad.

(viii) FLUIDO ELECTRICO

- **Situación: Corte del fluido eléctrico**
    - Comunicarse con la persona encargada del servicio eléctrico o el administrador del Edificio para saber las causas del corte de fluido eléctrico.
    - Si fuera corto circuito, el UPS mantendrá activo los servidores y algunas estaciones, mientras se repare la averia eléctrica.
    - Para el caso de apagón se mantendrá la autonomía de corriente que el UPS los brinda (corriente de emergencia).
    - Llámese corriente de emergencia a la brindada por el UPS.
    - Llámese corriente normal a la brindada por la compañía eléctrica.

- **Situación: Ante una inundación con corto circuito**
  - Paso 1: Bajar la llave principal eléctrico
  - Paso 2: Pedir el cierre de la llave general de agua.
  - Paso 3: Revisar Constantemente que el agua no llegue a la puerta de escape, en caso de cercanía del agua, evacuar inmediatamente o subir a superficie aislante.
  - Paso 4: En caso exista tiempo suficiente, se deberá enviar un mensaje o avisar vía telefónicamente (solo si el tiempo lo permite) advirtiendo el apagado de los servidores de la Municipalidad.
  - Paso 5: Se apagará la caja principal de corriente de la SGTIC.
  - Paso 6: En caso de encontrar artefactos eléctricos en el suelo, se levantarán sobre una superficie alta, para evitar su contacto con el agua.

(IX) CÁMARAS CIS

- **Situación: Perdida de señal entre las cámaras y centro de control de CIS.**
- Paso 1: Se verifica primero el enlace entre las radios, para verificar si es un problema de enlace o cámara.
- Paso 2: Problema es de enlace se va descartando cuál de los enlaces es el que tiene problemas.

(X) RADIO ENLACES

- **Situación: Falla del enlace principal de comunicaciones.**

  Falla del servicio de comunicaciones.
  Contingencia: Reemplazo de radio enlaces y antenas con características similares

(XI) CALL - CENTER

- **Situación: Falla en el equipo central de comunicaciones.**
  - Falla parcial o total del equipo central de la red LAN.
  - Contingencia: Reemplazo de central telefónica con características similares

(XII) BASE DE DATOS

- **Situación: Ante la falla general de alguno de los servidores principales, se procederá a levantar el servidor backup que corresponda.**
  - Paso 1: Ubicar el servidor backup correspondiente (Servidor de backup de base de datos)
  - Paso 2: Cambiar el IP del Servidor Backup por el del Servidor Principal.
  - Paso 3: Revisar que los servicios estén trabajando correctamente.
  - Paso 4: Comenzar con los trabajos de recuperación de Datos del Servidor Principal.
- **Situación: Error lógico de Datos**
  - Paso 1: Verificar el suministro de energía eléctrica. En caso de estar conforme proceder con el encendido del servidor y el levantamiento del Sistema Operativo.
  - Paso 2: Deshabilitar el ingreso de usuarios al sistema.
  - Paso 3: Descargar todos los volúmenes del servidor, a excepción del volumen raíz, de encontrarse este volumen con problemas, se deberá descargarlo también.
  - Paso 4: Cargar un utilitario que nos permita verificar en forma global el contenido del disco duro del servidor.
  - Paso 5: Al término de la operación de reparación se procederá a habilitar el acceso al sistema.

(XIII) WAN

- **Situación:** Falla en el equipo Firewall.
  - Falla parcial o total en el equipo Firewall
  - Contingencia: Se cuentas con contingencia automática de firewall.

(XIV) REDES DE DATOS

- **Situación: Identificación de virus** en una PC
  - Paso 1. Llamar al personal del Equipo de Plataforma Tecnológica
  - Paso 2: Sacar el Cable de Red de la PC comprometida
  - Paso 3: Pasar el antivirus que contenga la PC en ese momento
  - Paso 4: En caso el antivirus no elimine el virus, actualizar la versión o instalar un antivirus diferente.
    - En caso elimine el virus, realizar una actualización de la máquina.
    - En caso de no eliminarse el virus, revisar los puertos abiertos para la resolución de problemas / Utilización del Netstat), y contactarse con el administrador de red para ver si percibe alguna anomalía.
  - Paso 5: De no encontrarse en la Internet la solución al problema, se procederá a formatear la máquina comprometida.

- **Situación: Propagación de** un virus en la red
  - Paso 1: Llamar al personal del Equipo de Plataforma Tecnológica
  - Paso 2: Sacar el Cable de Red de las PC comprometidas para evitar el contagio del resto de PCs.
  - Paso 3: Pasar el antivirus que contenga la PC en ese momento
  - Paso 4: En caso el antivirus no elimine el virus, actualizar la versión o instalar un antivirus más potente.
    - En caso elimine el virus, realizar una actualización de la máquina.
    - En caso de no eliminarse el virus, revisar los puertos abiertos para la resolución de problemas / Utilización del Netstat), y contactarse con el administrador de red para ver si percibe alguna anomalía.
  - Paso 5: De no encontrarse en la Internet la solución al problema, se procederá a formatear todas aquellas máquinas comprometida.

e) Formación y funciones de los grupos de trabajo

El plan de contingencia detalla los diferentes niveles de toma de decisiones y acciones de respuesta ante cualquier situación que requiera la ejecución de un procedimiento de contingencia. De tal forma que las decisiones a tomar no dependan de consultas adicionales o que se generen dudas para su ejecución.

Así mismo, queda definido un comité de trabajo para el cumplimiento y actualización del Plan de Contingencias ante problemas informáticos, que participarán al momento de tomar decisiones ante eventualidades que impacten en el funcionamiento de los servicios informáticos de la GTIC.

f) Equipos o Brigada de Trabajo

El aspecto más importante de una organización para hacer frente a contingencias es la creación y entrenamiento de las brigadas o equipos de trabajo.

Estructura del equipo de trabajo o Brigada

Cada servicio de TI crítico identificado en el presente documento debe de contar con un equipo o brigada de trabajo designado por los miembros del comité de Seguridad, identificando sus miembros y responsabilidades concretas:

Jefe de brigada:	Miembro de brigadas:
Cargo:	Cargo:
Responsable:	Responsable:
Teléfono celular:	Teléfono celular:
Correo electrónico:	Correo electrónico:
Dirección:	Dirección:

A continuación, se detalla el procedimiento general de activación del Plan de Contingencias:

- Ante la detección de un desastre, el Equipo de Plataforma Tecnológica evaluará la magnitud de la misma e informará al Sub Gerente de Tecnologías de Información y Comunicaciones la ocurrencia de la misma y sus detalles.

- El Sub Gerente de Tecnologías de Información y Comunicaciones comunicará al Gerente Municipal la ocurrencia de la falla.

- El Sub Gerente de Tecnologías de Información y Comunicaciones dispone que los grupos de trabajo mencionados anteriormente se hagan presentes en sede central, a efectos de dar solución a la falla.

- El Equipo de Plataforma Tecnológica en conjunción con el Equipo de Desarrollo de Sistemas de Información coordinan la recuperación de los servicios afectados, de acuerdo a los procedimientos definidos para cada servicio o servidor.

- Se comunica al Sub Gerente de Tecnologías de Información y Comunicaciones que los servicios han sido recuperados, procediendo el mismo a verificar y dar la conformidad del caso.

- El Sub Gerente de Tecnologías de Información y Comunicaciones comunica al Gerente Municipal que el(os) servicio(s) afectados han sido recuperados y se procede a dar por cerrado el incidente.

Caso especial Brigada de emergencia (contra incendio/ primeros auxilios)

- Jefe de brigada

    - Comunicar de manera inmediata al Comité de Seguridad de la ocurrencia de una emergencia.

    - Estar al mando de las operaciones para enfrentar la emergencia cumpliendo con las directivas encomendadas por el Comité.

- Brigada de Emergencia (contra incendio / primeros auxilios):

  Producida una situación de emergencia:

  - Comunicar de manera inmediata al Comité de Seguridad de la ocurrencia de un incendio y actuar de inmediato haciendo uso de tos equipos contra incendio (extintores portátiles).

  - Al arribo de la Compañía de Bomberos informará las medidas adoptadas y las tareas que se están realizando, entregando el mando a los mismos y ofreciendo la colaboración de ser necesario.

  El responsable de la activación del Plan de Contingencias es el Sub Gerente de Tecnologías de Información y Comunicaciones, quien asume la conducción de los equipos de trabajos hasta lograr recuperar los servicios afectados

Lista de Personas de la SGTIC

Directorio telefónico del personal considerado esencial para la organización en esas situaciones críticas, incluyendo el personal encargado de realizar medidas preventivas y los responsables para las acciones de la recuperación y preparación de medios alternativos, ver anexo 11 correspondiente.
Con la finalidad de realizar las comunicaciones rápidas con los proveedores de servicios del recurso, incluso con los fabricantes, vendedores o abastecimiento, ver anexo 12 correspondiente.

g) Resumen de principales componentes del plan de contingencias.

En el siguiente cuadro se muestran el principal riesgo de cada uno de ellos y su correspondiente estrategia de contingencia.

Área afectada	Riesgos identificados	Impacto	Probabilidad de falla	Prioridad	Estrategia de Contingencia
Todas las Áreas	Falla de Servidor	Alto	Baja	1	Servidor de Respaldo
Locales Periféricos	Falla Red Interlocal	Alto	Baja	1	Cambio de Antenas
Todas las Áreas	Falla de servicio de Telefonía	Alto	Baja	1	Cambio de Central telefónica
Todas las Áreas	Servicio de Internet	Alto	Baja	1	Contactar con proveedor
Oficinas	Falla Infratuctura de red	Medio	Baja	2	Reparación o cambio de Cableado Estructura
Todas las Áreas	Falla de Estación de trabajo	Medio	Alta	3	Reparación o cambio de Estación de Trabajo

IV.PLAN DE PRUEBAS

Objetivos

- Verificar si los procedimientos de contingencias funcionan adecuadamente, en el momento de afrontar un desastre y dentro de los periodos de recuperación especificados.
- Estimar y/o identificar los recursos necesarios en el momento de ocurrencia de una contingencia

Planificación

Los siguientes aspectos deben ser considerados en la etapa de planificación de las pruebas:

Fecha y Hora

La fecha y hora para la ejecución de las pruebas será establecida por el Sub Gerente de Tecnologías de Información y Comunicaciones.

Revisión

Los procedimientos de recuperación de servicios serán revisados por cada uno de los miembros que participaran en el proceso de implementación del plan de pruebas y deben de ser discutidos por lo menos dos días antes de la fecha a llevarse a cabo.

Responsabilidades

El Sub Gerente de Tecnologías de Información y Comunicaciones quien liderará la ejecución de las pruebas asignará responsabilidades a cada uno de los miembros tomando en cuenta las actividades a realizar.

Se asignará un responsable encargado de tomar los tiempos utilizados en cada actividad durante el proceso, el cual se plasmará en un cuadro de actividades y tiempos.

Método

El método de pruebas a utilizar es el llamado "Método de Prueba Especifica", el cual fue considerado el más adecuado debido a que este se realiza por cada operación critica identificada y se basa en el procedimiento de contingencia definido para cada servicio.

Recursos

Para realizar el plan de pruebas es necesario contar con los siguientes recursos:

Equipos que cuenten con similares características a los equipos que se encuentran actualmente en producción.

El personal necesario para la ejecución de este plan de pruebas, es el personal técnico del equipo de plataforma tecnológica y proveedores de servicios.

Casos de prueba

El Equipo de Plataforma Tecnológica definirá en la etapa de revisión del Plan de Pruebas en los casos de pruebas definidos para verificar el funcionamiento de los procedimientos de contingencia desarrollados. En cada caso se especifican los tiempos estimados por

cada actividad, recursos y el orden de restauración de los servicios, en caso de que más de uno fuese afectado.

Aprobación de resultados de verificación

Como prueba final, El Sub Gerente de Tecnologías de Información y Comunicaciones, deberá de comprobar de manera integra, la operatividad de cada uno de los servicios críticos afectados, para que, otorgue su aprobación y de esta manera dar por concluida la prueba de contingencia.

RELAVISTA CONFÍA en U	ANEXO 01 "INVENTARIO DE COMPUTADORAS Y PORTATILES"								V.1	
	SUBGERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN								Elaborado por: SGTIC	
NOMBRE	ESTADO	FABRICANTE	TIPO	MODELO	SISTEMA OPERATIVO	UBICACIÓN	USUARIO	CARACTERISTICAS	IP	ANTIVIRUS

MUNICIPALIDAD DISTRITAL DE RELAVISTA

BELLAVISTA confía en ti	ANEXO 02-A "INVENTARIO DE PERIFERICOS - MONITORES"	V.1
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNIACION	Elaborado por : SGTIC

FABRICANTE	UBICACIÓN	ESTADO	MODELO	SERIAL	USUARIO

BELLAVISTA confía en ti	ANEXO 02-B "INVENTARIO DE PERIFERICOS - ANEXOS	V.1
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES	Elaborado por : SGTIC

SIP	ESTADO	FABRICANTE	UBICACIÓN	MODELO	USUARIO	IP

BELLAVISTA confía en ti	ANEXO 02-C "INVENTARIO DE PERIFERICOS - IMPRESORAS"	V.1
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIONES	Elaborado por : SGTIC

NOMBRE	ESTADO	FABRICANTE	UBICACIÓN	TIPO	MODELO	SERIAL	IP

BELLAVISTA confía en ti	ANEXO 03 "INVENTARIO DE CAMARAS"		V.1	
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION		Elaborado por :	SGTIC

LOCAL	PISO	UBICACION	DISPOSITIVO	MARCA	TIPO	FORMA	GRABA EN	AÑO

BELLAVISTA confía en ti	ANEXO 04 "INVENTARIO DE EQUIPOS DE COMUNICACIÓN Y DATA"	V.1	
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION	Elaborado por :	SGTIC

LOCAL	PISO	UBICACIÓN	NOMBRE DE EQUIPO	MARCA	PUERTOS	MODELO	ADMINISTRABLE	TIPO	ESTADO	AÑO COMPRA

BELLAVISTA onfía en ti	ANEXO 05 "INVENTARIO DE SERVIDORES"	V.1	
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION	Elaborado por :	SGTIC

#	AMBITO	FUNCIONALIDAD	APLICATIVO	SISTEMA OPERATIVO	TIPO	DISCO	MEMORIA	PROCESADOR	MARCA	MODELO	AÑO COMPRA

ruaVISTA confía en ti	ANEXO 06 "INVENTARIO BD Y SISTEMAS"	V.2
	SUBSECRETARÍA DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIÓN	Elaborado por: SGTIC

SISTEMA/APLICACIÓN/MODULO	GESTOR DE BASE DE DATOS	LENGUAJE DE PROGRAMACION	UNIDAD ORGANICA RESPONSABLE	PROPIEDAD	BASE DE DATOS	DESCRIPCION	SERVIDOR DE INSTALACION	RESPONSABLE

BELLAVISTA confía en ti	ANEXO 07-A "INVENTARIO DE LICENCIAS DE SOFTWARE"	V.1	
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNIACION	Elaborado por:	SGTIC

IP	SOFTWARE	CANTIDAD	UBICACIÓN

BELLAVISTA confía en ti	ANEXO 07-B "INVENTARIO DE LICENCIAS DE SOFTWARE" V1	
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION	Elaborado por: SGTIC

IP	SOFTWARE	TIPO DE USO	CANTIDAD	UBICACIÓN

BELLAVISTA confía en ti	ANEXO 08 "INVENTARIO DE DOMINIO"	v.1	
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNIACION	ELABORADO POR	SGTIC

SERVIDOR	TIPO	NOMBRE	ZONA	PROVEEDOR/ REGISTRO

BELLAVISTA confía en ti	ANEXO 09 "INVENTARIO DE EQUIPOS DE RED CORPORATIVA"	V1
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION	Elaborado por: SGTIC

DISPOSITIVO	PROPIETARIO	MARCA	MODELO

BELLAVISTA confía en ti	ANEXO 10 "PERIOCIDAD DE LOS BACKUP"	V.1
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION	Elaborado por: SGTIC

SERVICIO	PERIODICIDAD	UBICACIÓN DE BACKUP

BELLAVISTA confía en ti	ANEXO 11 "LISTADO DE PROVEEDORES"	V.1	
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION	Elaborado por :	SGTIC

SERVICIO	PROVEEDOR	CONTATO	CARGO	NUMERO1	NUMERO2	CORREO

MUNICIPALIDAD DISTRITAL DE BELLAVISTA
V°B°

BELLAVISTA confía en ti	ANEXO 12 "LISTADO DE PERSONAL ANTE EMERGENCIAS"			V.1	
	SUBGERENCIA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACION			Elaborado por :	SGTIC
COMITÉ DE TRABAJO PARA EL CUMPLIMIENTO Y ACTUALIZACION DEL PLAN DE CONTINGENCIA					
CARGO	NOMBRES Y APELLIDOS	TELEFONO	CORREO	FUNCIONES	
COMITÉ DE SEGURIDAD					
CARGO	RESPONSABLE	TELEFONO	CORREO	FUNCIONES	