

**DECRETO APRUEBA PROCEDIMIENTO DE
GESTIÓN DE INCIDENTES DEL
DEPARTAMENTO DE TECNOLOGÍAS DE
INFORMACIÓN Y COMUNICACIÓN DE LA
MUNICIPALIDAD DE LO BARNECHEA.**

DECRETO DAL N°1341/2021

LO BARNECHEA, 01-12-2021

VISTOS: lo dispuesto en el D.S. N°81, de 2005 del Ministerio Secretaría General de la Presidencia (SEGPRES), que aprueba norma técnica para los órganos de la Administración del Estado sobre la seguridad y confidencialidad de los documentos electrónicos, la norma chilena NCh-ISO 27001:2013, sobre sistema de gestión de seguridad de la información; y, en uso de las facultades que me confiere el artículo 56 y 63° letra i) de la citada Ley N°18.695, Orgánica Constitucional de Municipalidades, y;

TENIENDO PRESENTE:

- a) La necesidad de contar con un procedimiento decretado, que proporcione el marco de acción ante un incidente declarado, tanto en las Plataformas como en los Sistemas de la Municipalidad de Lo Barnechea.
- b) Que, resulta necesario contar con políticas específicas, procedimientos detallados e instructivos acuciosos, que permitan articular el sistema, integrándose, tanto de manera metodológica como documental, con los sistemas de gestión institucionales.
- c) Que, mediante el informe N°407, 409 y 410, la Contraloría General de la República, observo debilidades en la gestión de incidentes y problemas tecnológicos. Generando la necesidad de contar con un procedimiento que realizara la gestión de los incidentes generados, tanto en las Plataformas como en los Sistemas de la Municipalidad de Lo Barnechea.

DECRETO

1. **APRUÉBASE** Procedimiento de Gestión de Incidentes. Que a continuación se transcribe:

-----xxxxxXXXXXxxxxx-----

PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
MUNICIPALIDAD DE LO BARNECHEA

VERSIÓN	FECHA	ELABORADO	REVISADO	MODIFICACIONES
1.0	07/04/2021	ROlivares	IDaroch	Documento Original
1.1	15/11/2021	ROlivares	SToledo	Actualización

TABLA DE CONTENIDO

1. OBJETIVOS.
2. ROLES Y RESPONSABILIDADES.
3. DEFINICIÓN.
4. ALCANCE.
5. PROCEDIMIENTO.
 - 5.1. DESCRIPCIÓN DEL PROCEDIMIENTO DE GESTIÓN DE INCIDENTES.
 - 5.2. FLUJO PROCEDIMIENTO DE GESTIÓN DE INCIDENTES.
6. CIERRE DE UN INCIDENTE.
7. MEJORA CONTINUA.
8. ALMACENAMIENTO.
9. IMÁGENES DEL SISTEMA DE REGISTRO Y ADMINISTRACIÓN DE INCIDENTES.
10. ANEXO: INFORME DE INCIDENTE.
11. ANEXO: EJEMPLO INFORME DE INCIDENTE.

1. OBJETIVOS.

En el presente documento se establece el procedimiento que debe seguir el personal del Departamento de Tecnologías de Información y Comunicación de la Municipalidad de Lo Barnechea, con la finalidad de reaccionar de forma correcta ante un Incidente generado en sus sistemas o plataformas, el cual comprometa el correcto funcionamiento de uno o más componentes de la infraestructura Municipal.

2. ROLES Y RESPONSABILIDADES.

- ✓ **Usuario MLB:** persona que informa un requerimiento a Soporte, el cual puede ser catalogado como un Incidente.
- ✓ **Supervisor de la Mesa de Soporte:** funcionario que gestiona y categoriza los requerimientos ingresados por distintos canales a la mesa de Soporte de la Municipalidad de Lo Barnechea. será el encargado de identificar los requerimientos que reúnan las características para ser catalogados como un incidente.
- ✓ **Encargado de Continuidad Operativa (ECO):** funcionario encargado de garantizar la continuidad operativa de las plataformas e infraestructura de la Municipalidad de Lo Barnechea. Será el encargado de realizar las gestiones necesarias para solventar el incidente declarado, realizando gestiones con el equipo interno y con los proveedores externos, con la finalidad de solucionar el incidente, además será el encargado de gestionar, informar y documentar el incidente.
- ✓ **Especialista Interno:** Profesional perteneciente al Departamento TIC que administra y gestiona sistemas o plataformas específicas dentro de la estructura organizacional del Departamento.

- ✓ **Especialista Externo:** Profesional perteneciente a empresa externa que presta servicios específicos a la Municipalidad de Lo Barnechea.

3. DEFINICIÓN.

A continuación, se realiza la definición y diferenciación entre los conceptos de requerimiento e Incidente.

REQUERIMIENTO	Corresponde a todas las solicitudes realizadas por los usuarios a la mesa de soporte de la Municipalidad de Lo Barnechea, ingresadas mediante sus canales de comunicación, correo electrónico (soporte@lobarnechea.cl), anexo telefónico (+56228273701)
INCIDENTE	Evento que no forma parte usual o normal de la operación diaria del proceso de negocio, que causa o puede causar una interrupción o reducción en la calidad del servicio. Todo incidente ingresa a la mesa de soporte como un requerimiento, el cual se categoriza como incidente debido al análisis cualitativo y cuantitativo realizado por el supervisor de la mesa.

4. ALCANCE.

Este procedimiento es de carácter interno y aborda la gestión de Incidentes en Sistemas, Plataformas e Infraestructura TIC de la Municipalidad de Lo Barnechea. dicho procedimiento se encuentra regulado por las normativas definidas por la Municipalidad, tanto a nivel de infraestructura, servicios y seguridad de la información.

5. PROCEDIMIENTO.

A continuación, se detalla el procedimiento que se debe ejecutar para gestionar los incidentes generados en los sistemas, plataformas o infraestructura TIC de la Municipalidad de Lo Barnechea.

5.1. DESCRIPCIÓN DEL PROCEDIMIENTO DE GESTIÓN DE INCIDENTES.

Una vez declarado un incidente o haber identificado la posibilidad de que ocurra uno, se deberá proceder de manera inmediata con las siguientes acciones:

- I. El Supervisor de la Mesa de Soporte o quien lo subrogue, una vez declarado el incidente o haber identificado la posibilidad de que ocurra uno, deberá notificar a la brevedad posible al Encargado de Continuidad Operativa (ECO) o quien lo subrogue, además de realizar la asignación del incidente o su registro en el sistema de Gestión de Requerimientos.

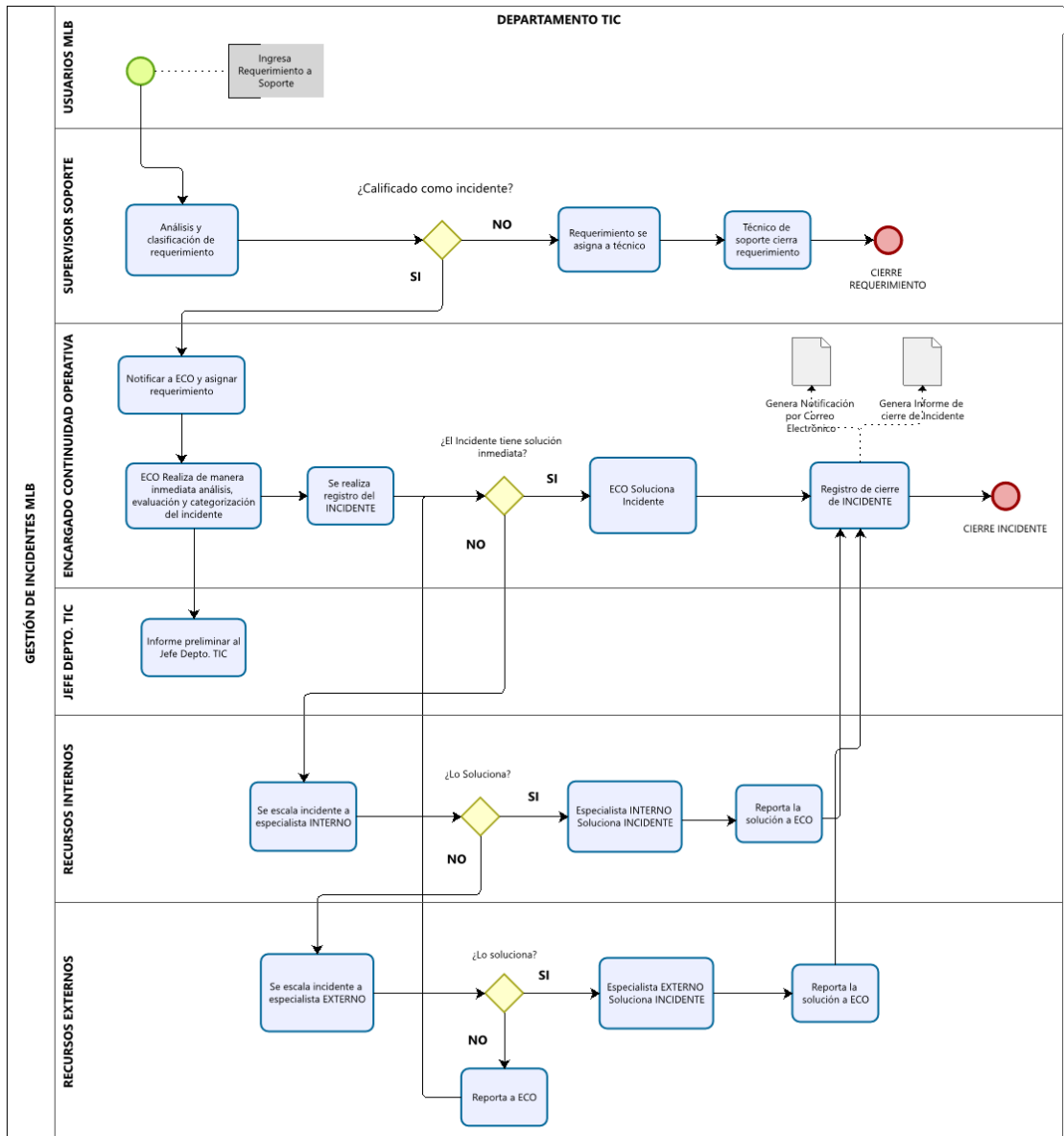
**ALCALDIA
SECRETARÍA COMUNAL DE PLANIFICACIÓN
DEPTO. DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN**

- II. El Encargado de Continuidad Operativa deberá realizar de manera inmediata un análisis y evaluación del incidente, definiendo las acciones que se deberán ejecutar para gestionar la solución del incidente.
- III. El Encargado de Continuidad Operativa deberá informar de manera inmediata y de forma preliminar al jefe del Depto. TIC, de la declaración de un incidente, entregando un reporte con la información que maneja hasta el minuto.
- IV. El Encargado de Continuidad Operativa deberá realizar el registro de todas las gestiones internas y externas desarrolladas en el marco del proceso de solución de un incidente, esto con la finalidad de gestionar, informar y documentar el incidente. Se deberá considerar como mínimo la siguiente información:
 - ✓ Descripción del incidente.
 - ✓ Posible causa del incidente.
 - ✓ Identificación de responsables técnicos.
 - ✓ Estimación de tiempos de respuesta.
 - ✓ Seguimiento del incidente.
 - ✓ Solución de incidente.
 - ✓ Cuantificación del incidente.
 - ✓ Monitoreo del incidente.
- V. Todas las acciones y comunicaciones generadas como respuestas al incidente declarado deberán incluir las siguientes definiciones, esto con el objetivo de mejorar el desempeño de la gestión y atención del incidente generado:
 1. Una vez verificado el Incidente y de la manera más rápida posible, se deberá recopilar toda la evidencia asociada.
 2. Se deberá calificar el incidente de acuerdo con su origen y sistemas o plataformas afectadas.
 3. Clasificar el nivel de URGENCIA Y CRITICIDAD del incidente de acuerdo con la siguiente tabla:

Nivel	Descripción
Bajo	Incidente de impacto bajo, no afecta la continuidad operativa.
Medio	Incidente de impacto medio, se encuentra afectada la continuidad operativa de manera localizada y circunscrita a ciertos sistemas y plataformas.
Alto	Incidente de impacto Alto, se encuentra afectada la continuidad operativa de sistemas e infraestructuras TIC municipales.
Critico	Incidente de impacto Critico, se encuentra afectada la continuidad operativa de la totalidad de los sistemas e infraestructuras TIC municipales.

4. Efectuar un escalamiento urgente a niveles superiores, según la pertinencia y relevancia del incidente.
5. Asegurarse de que todas las actividades de respuesta y gestión se registren correctamente, esto con la finalidad de realizar un análisis posterior.

5.2. FLUJO PROCEDIMIENTO DE GESTIÓN DE INCIDENTES.



6. CIERRE DE UN INCIDENTE.

Una vez que el incidente se encuentre bajo control el Encargado de Continuidad Operativa debe registrar el cierre del incidente en el sistema de Gestión de Requerimientos, notificando a todos los involucrados y afectados el cierre del incidente. Además de lo anterior, se deberá generar un informe que consigne todos los antecedentes del incidente ocurrido, definiendo: quien lo reportó, la causa, la criticidad del incidente, la solución ejecutada y la fecha en la que el incidente quedó bajo control. Este informe debe ser enviado al Jefe del Depto. TIC, Director Secpla. y Administrador Municipal.

7. MEJORA CONTINUA.

El Encargado de Continuidad Operativa deberá recopilar toda la información y conocimiento obtenido gracias al análisis y posterior solución y/o mitigación del incidente y junto al Encargado de la Seguridad de la Información y al jefe Depto. TIC. Deberán generar un informe, el cual será disponibilizado como base de conocimiento

para todos los funcionarios del Depto. TIC, lo anterior con el propósito de generar un aprendizaje, además de ayudar a reducir la probabilidad e impacto de los futuros incidentes que se pudiesen generar.

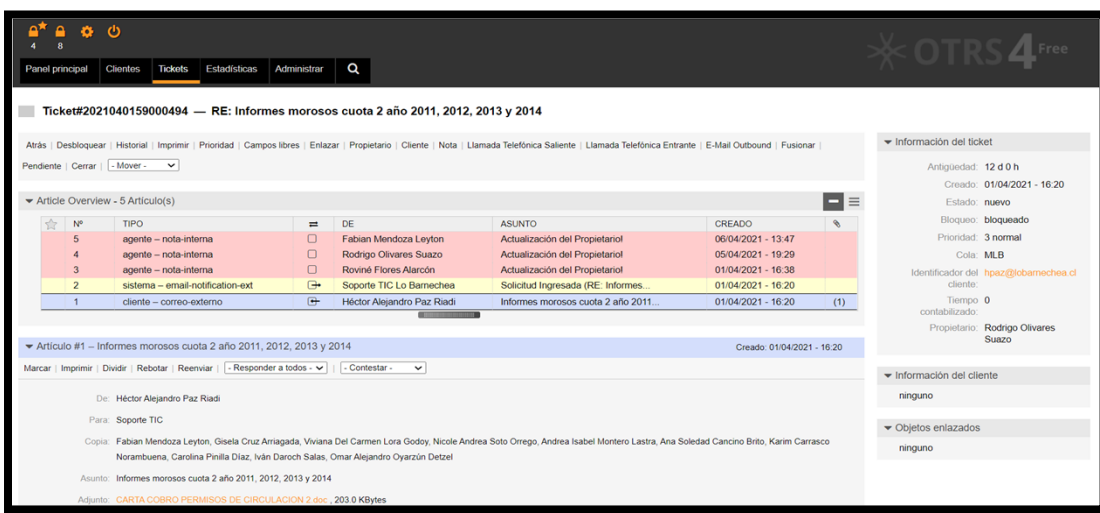
8. ALMACENAMIENTO.

Toda la documentación asociada al proceso de Gestión de Incidentes deberá estar almacenada en una carpeta dentro de la estructura documental del Departamento de Tecnologías de Información y Comunicación.

RUTA: \\vmshare\DataSecplan\Depto. TIC\GESTION DE INCIDENTES__

9. IMÁGENES DEL SISTEMA DE REGISTRO Y ADMINISTRACIÓN DE INCIDENTES.

✓ VISTA GENERAL INCIDENTE.

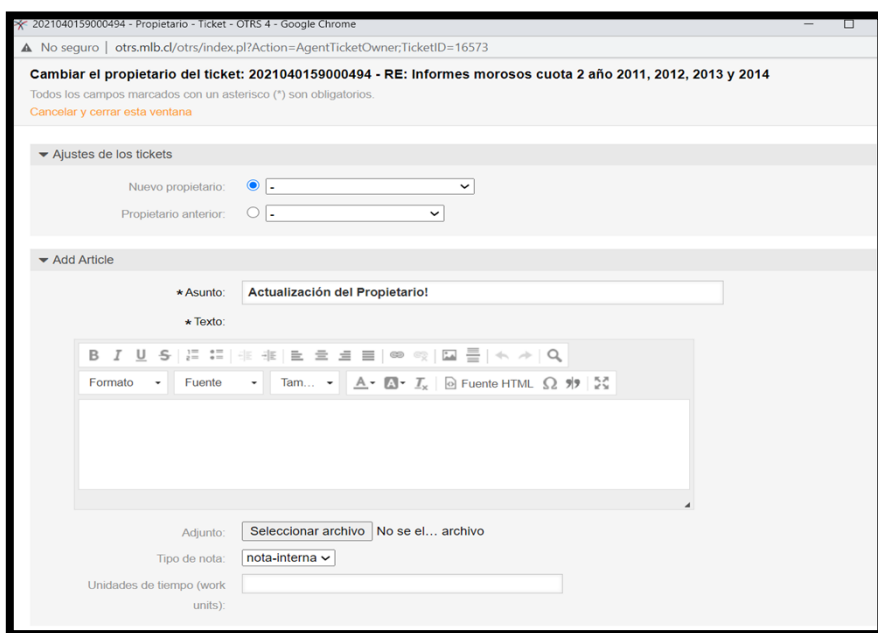


The screenshot shows the OTRS 4 Free interface. The main header includes navigation tabs: Panel principal, Clientes, Tickets, Estadísticas, and Administrar. The current view is 'Ticket#2021040159000494' with the subject 'RE: Informes morosos cuota 2 año 2011, 2012, 2013 y 2014'. Below this is a table of articles:

Nº	TIPO	DE	ASUNTO	CREADO
5	agente - nota-interna	Fabian Mendoza Leyton	Actualización del Proprietario	06/04/2021 - 13:47
4	agente - nota-interna	Rodrigo Olivares Suazo	Actualización del Proprietario	05/04/2021 - 19:29
3	agente - nota-interna	Roviné Flores Alarcón	Actualización del Proprietario	01/04/2021 - 16:38
2	sistema - email-notification-ext	Soporte TIC Lo Barnechea	Solicitud Ingresada (RE: Informes...	01/04/2021 - 16:20
1	cliente - correo-externo	Héctor Alejandro Paz Riadi	Informes morosos cuota 2 año 2011...	01/04/2021 - 16:20 (1)

Below the table, the details of Article #1 are shown, including the sender (Héctor Alejandro Paz Riadi), recipient (Soporte TIC), and subject (Informes morosos cuota 2 año 2011, 2012, 2013 y 2014). The right sidebar provides additional information about the ticket, such as its age (12 d 0 h), creation date (01/04/2021 - 16:20), and status (nuevo).

✓ CAMBIO DE PROPIETARIO DEL INCIDENTE.



The screenshot shows the 'Cambiar el propietario del ticket' form in the OTRS 4 Free interface. The form is titled 'Cambiar el propietario del ticket: 2021040159000494 - RE: Informes morosos cuota 2 año 2011, 2012, 2013 y 2014'. It includes a section for 'Ajustes de los tickets' with dropdown menus for 'Nuevo propietario' and 'Propietario anterior'. Below this is the 'Add Article' section, which contains a text area for the subject and a rich text editor for the message body. The subject is currently set to 'Actualización del Propietario!'. There is also a section for 'Adjunto' with a 'Seleccionar archivo' button and a 'Tipo de nota' dropdown set to 'nota-interna'.

✓ **ASIGNAR PRIORIDAD AL INCIDENTE.**

Cambiar la prioridad del ticket: 2021040159000494 - RE: Informes morosos cuota 2 año 2011, 2012, 2013 y 2014
Todos los campos marcados con un asterisco (*) son obligatorios.
[Cancelar y cerrar esta ventana](#)

▼ Ajustes de los tickets

Prioridad: 3 normal ▼

▼ Add Article

* Asunto:

* Texto:

B I U S | | **Fuente** | **Tam...** | **A** | **A** | **Ix** | **Fuente HTML** |

Adjunto: No se el... archivo

Tipo de nota: ▼

Unidades de tiempo (work units):

✓ **DOCUMENTAR UN INCIDENTE**

Añadir una nota al ticket: 2021040159000494 - RE: Informes morosos cuota 2 año 2011, 2012, 2013 y 2014
Todos los campos marcados con un asterisco (*) son obligatorios.
[Cancelar y cerrar esta ventana](#)

▼ Add Article

* Asunto:

* Texto:

B I U S | | **Fuente** | **Tam...** | **A** | **A** | **Ix** | **Fuente HTML** |


Adjunto: No se el... archivo

Tipo de nota: ▼

Unidades de tiempo (work units):

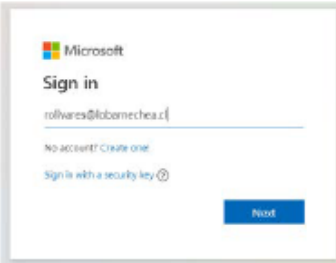
Enviar

11. ANEXO: EJEMPLO INFORME DE INCIDENTE.



LoBarnechea
JUNTOS HACEMOS UNA COMUNA MEJOR

INFORME INCIDENTE
DEPARTAMENTO TIC

Fecha:	11 de mayo 2021
Hora:	17:15 Hrs.
Origen Incidente:	Alerta de Servicio Exchange, degradación del servicio.
Descripción:	Problema afecta la visualización del contenido del correo electrónico en Outlook.
Impacto para usuario:	Es posible que los usuarios no puedan ver el contenido de los mensajes de correo electrónico en Outlook.
Medidas de Mitigación:	<p>los informes iniciales indican que Outlook web no se ve afectado, por lo cual los usuarios pueden acceder a esta plataforma para poder revisar los mensajes de correo electrónico mientras se soluciona el incidente.</p> <p>Paso 1. Ingresar a la URL de la página de la Municipalidad de Lo Barnechea.</p> <p>Paso 2. Ingresar al final de pagina web a la opción Web Mail.</p> <div style="border: 1px solid black; background-color: #1a3d4d; color: white; padding: 5px; text-align: center; margin: 5px 0;"> <p>PAGO PATENTES COMERCIALES</p> <p>WEB MAIL</p> <p>TRABAJA CON NOSOTROS</p> <p>RECURSOS HUMANOS</p> <p>CERTIFICADOS DE HONORARIOS</p> <p>ESCRITORIO CONCEJALES</p> <p>RIM MÓVIL</p> <p>PAGO PROVEEDORES</p> </div> <p>Paso 3: Ingresar usuario y contraseña de correo electrónico (es la misma del usuario del equipo).</p> <div style="border: 1px solid gray; padding: 10px; margin: 5px 0;">  </div>
Próxima actualización:	19:00 hrs.

Actualización de Incidente	
Fecha:	11 de mayo 2021
Hora:	19:15 Hrs.
Estado Actual:	<p>El proveedor del servicio (Microsoft) ha identificado la causa subyacente del incidente y está aplicando una solución. Esta solución llegará a todos los usuarios afectados de forma incremental en el transcurso de las próximas cuatro a cinco horas.</p> <p>Una vez que los usuarios reciban la corrección, deberán reiniciar su cliente de correo electrónico para aplicar dicha corrección. En algunos casos es posible que los usuarios necesiten reiniciar su cliente por una segunda vez para que los cambios surtan efecto.</p> <p>Se espera solventar este proceso y restaurar el servicio para todos los usuarios afectados antes de las 03:00 AM del 12 de mayo de 2021.</p>
Medidas de Mitigación:	Los usuarios afectados pueden seguir utilizando las soluciones alternativas descritas anteriormente.
Causa del Incidente:	Microsoft informa que la causa del incidente radica en una actualización reciente en los sistemas que facilitan la administración de visualización de texto para el contenido dentro del cliente de Outlook.
Próxima actualización:	08:30 AM – miércoles 12 de mayo 2021.

Actualización de Incidente	
Fecha:	12 de mayo 2021
Hora:	08:50 AM
Estado Actual:	El proveedor del servicio (Microsoft) ha informado que el incidente se encuentra resuelto con éxito, se informa que pueden existir usuarios que para solucionar el problema deban reiniciar su cliente de correo electrónico.
Causa del Incidente:	<p>Preliminarmente Microsoft informó que la causa del incidente fue una actualización en los sistemas que facilitan la administración de visualización de texto para el contenido dentro del cliente de Outlook.</p> <p>El proveedor está realizando un análisis completo de la causa raíz y se proporcionarán detalles adicionales en el informe final de cierre del incidente. El que será publicado dentro de los próximos cinco días hábiles.</p> <p>El proveedor está realizando una revisión exhaustiva de su codificación con la finalidad de comprender cómo ocurrió el problema y por qué se pasó por alto durante las pruebas y el ciclo de implementación inicial.</p>
Cierre de Incidente:	09:00 AM – miércoles 12 de mayo 2021.

-----xxxxxXXXXXxxxxx-----

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE

VIVIAN BARRA PEÑALOZA
SECRETARIO MUNICIPAL
MUNICIPALIDAD DE LO BARNECHEA

JUAN CRISTOBAL LIRA IBAÑEZ
ALCALDE
MUNICIPALIDAD DE LO BARNECHEA

Este documento incorpora Firma(s) Electrónica(s) Avanzada(s)

