Manual de procedimientos internos administrativos

Procedimiento para solucionar fallas en el servicio de correo electrónico
MPIA-DTI-183
Revisión Original

Procedimiento para solucionar fallas en el servicio de correo electrónico

1. Control

1.1. Tabla de autorizaciones

No. de Revisión	Emitido por	Autorizado por
Original	Camilo Luna / Director de Tecnología de Información	Víctor Manuel Landa Reyes / Director de Seguridad Aérea y Aseguramiento de la Calidad

1.2. Registro de revisiones

No. de Revisión	Fecha de la Revisión	Motivo de la Revisión
Original	Mayo 2021	Edición original

1.2.1. Responsable de la revisión

El responsable de editar, revisar y actualizar el presente procedimiento es el Director de Tecnología de Información.

1.2.2. Criterio de la revisión

Este procedimiento será revisado cuando menos una vez al año a partir de la fecha su emisión, o antes si se cambia para mejorar el sistema administrativo de la organización, o bien, a causa de la generación o actualización de la regulación aplicable.

1.3. Lista de distribución

- Dirección de Tecnología de Información
- Suplente

2. Contenido

2.1. Definiciones y acrónimos

Phising: Envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza pero que en realidad pretenden manipular al receptor para robar información confidencial. Esto genera una cantidad enorme de mansajes que degradan el rendimiento del servidor donde opera este servicio hasta el punto de dejar de funcionar.

2.2. Objetivo

Hacer del conocimiento de la Dirección de Tecnología de Información, así como el personal que designe alternativo responsable, de la forma de recuperar el servicio de Correo Electrónico en caso de que dicho servicio presente considerable lentitud o incluso deje de estar accesible.

2.3. Alcance

Personal de la Dirección de Tecnología de Información, así como quien la misma designe se haga cargo de aplicar este procedimiento en caso de ausencia.

2.4. Responsabilidades

Director de Tecnología de Información

1. Es responsable de mantenerse actualizado, de la manera que le parezca conveniente, para poder gestionar correctamente el servicio de correo electrónico y tener la capacidad de solucionar los posibles problemas que se presenten en el servicio.

Suplente

1. Es responsable de llevar a cabo las tareas indicadas en el presente procedimiento en caso de ausencia del Director de Tecnología de Información, para mantener la operatividad del servicio de correo electrónico dentro de la organización.

2.5. Referencias

NA

2.6. Descripción del procedimiento

2.6.1. Para purgar el servicio que ha sufrido alguna clase de ataque pishing

Paso	Responsable	Descripción
1	Director de TI / Suplente	Acceder al al servidor que opera el Correo Electrónico de TAR a través de la herramienta llamada Webmin: https://server2.tarmexico.com:10000.
2	Director de TI / Suplente	Ingresar el usuario “root” y contraseña “xxxxxx” (este es de uso exclusivo de la Dirección de Tecnología de Información y de quien haya designado alternativo)
3	Director de TI / Suplente	En la pantalla principal de webmin, que se ha desplegado como resultado del paso anterior, identificar el menú desplegable a la izquierda de la pantalla y seleccionar la opción “Servers”/“Postfix Mail Server”.
4	Director de TI / Suplente	Seleccionar la opción “Mail Queue” en la parte inferior derecha de la ventana.
5	Director de TI / Suplente	Identificar cual es la cuenta afectada. Esto podrá verse facilmente ya que de esa cuenta estarán saliendo gran cantidad de mensajes.
6	Director de TI / Suplente	Cambiar la contraseña de la cuenta identificada en el paso anterior siguiendo el procedimiento MPIA-DTI-184 Guía para la administración del servicio de correo electrónico.
7	Director de TI / Suplente	Volver a la pantalla donde se tiene abierta la opción de “Mail Queue” (paso 4) y seleccionar la opción “Find Queued Messages where”.
8	Director de TI / Suplente	Ingresar la cuenta de correo afectada, primero con la opción [From: matches] en el campo siguiente poner la cuenta del problema (solo lo anterior al @) y [search].
9	Director de TI / Suplente	En la lista que se ha desplegado resultado del paso anterior, ir hasta debajo de la lista y dar clic en la opción ¨Select all¨ y posteriormente eliminarlos con el botón “Delete Selected Messages”.
10	Director de TI / Suplente	Verificar en la opción de “Mail Queue” que los mensajes han sido eliminados.
11	Director de TI / Suplente	Realizar de nuevo los pasos 7, 8 9 y 10, pero ahora con la opción ¨Find Queued Messages where¨ y [To: matches].
12	Director de TI / Suplente	Salir del servidor seleccionando la opción “Logout” en la parte inferior del menú ubicado en la parte inferior izquierda.
13	Director de TI / Suplente	Ingresar a la cuenta de correo afectada vía Web a través de la página webmail.tarmexico.com, con la nueva contraseña establecida en el paso 6.
14	Director de TI / Suplente	Una vez que se desplieguen los mensajes contenidos en ¨Inbox¨, en la parte inferior de esta ventana hay una caja que dice ¨Select¨ dar clic en ¨All¨ y en la parte superior seleccionar la opción ¨Delete¨ con lo que se eliminará todo mensaje en dicha bandeja, eliminando así la posibilidad que el ataque continúe.
15	Director de TI / Suplente	Contactar al usuario de la cuenta afectada e informarle a cerca de su nueva contraseña y que no debe abrir archivo anexo alguno en mensajes de los que desconoce el remitente ya que su cuenta se vio afectada y se perdió todo mensaje en ella.
16	Director de TI / Suplente	Esperar 15 minutos y revisar si el servicio de correo electrónico se ha normalizado. En caso de ser así, el proceso acaba en el presente paso. De no ser así, seguir al paso 17.

Paso	Responsable	Descripción
17	Director de TI / Suplente	Repetir paso 1 y 2.
18	Director de TI / Suplente	En la pantalla principal de webmin que se ha desplegado como resultado del paso anterior, identificar el menú desplegable a la izquierda de la pantalla y seleccionar la opción “System”/“Bootup Shutdown”.
19	Director de TI / Suplente	En la serie de servicios que se han desplegado como resultado del paso anterior, dar clic en la opción “Reboot System”, confirmar la acción y esperar un lapso de 10 a 15 minutos para que el servidor se reinicie.

2.7. Documentos aplicables y/o anexos

NA