Manual de crisis de sitios web Remington.

Introducción.

El siguiente manual de crisis se realiza para estar preparados en cualquier situación que se presente y que altere la reputación del sitio Web de Uniremington.

Definir un protocolo para manejar las crisis del sitio Web tiene sentido en la medida en que permitirá cuidar la “imagen” de las entidades y evitar que una comunidad dispuesta a escuchar e interactuar, se convierta en una comunidad tóxica anclada en la crítica destructiva.

Por lo anterior, se crea un manual que permita la comunicación que mantenga el protocolo en los diferentes canales digitales.

Objetivos.

Objetivo general.

Establecer un protocolo de crisis para el sitio web y los micro sitios Uniremington, donde se tomen a tiempo acciones que permita mantener la información para la comunidad.

Objetivos específicos.

- Lograr recuperar a tiempo: sitio web, micro sitios o landings que puedan presentar inconvenientes.
- Estimar un Backup o respaldo de la última versión del sitio para así poder reestablecerlos a la menor brevedad posible.
- Tener presente los cambios realizados durante el último mes para al momento de la restauración no se pierda la información.

Destinatarios del protocolo.

Este protocolo es un documento de consulta para todas las personas que tengan relación directa con el manejo de los sitios web Uniremington, quienes pueden ser: Web master, Auxiliar Web master o cualquier persona que esté relacionada con este tema.

¿Qué es una crisis en los sitios web?

a) La caída del servidor Uniremington.
b) Un error de código
c) Un ataque informático por parte hacker.

¿Pasos para la solución de una crisis en sitio web?

a) La caída del servidor Uniremington.

Medidas preventivas para evitar una caída del servidor: La mejor manera de evitar un fallo en el servidor es adelantarse a riesgos específicos mediante medidas de seguridad informática enfocadas a la protección de la infraestructura computacional y que tienen relación, por regla general, con una serie de acciones infraestructurales y organizativas que afectan a la elección y al diseño del lugar donde se instalan los servidores.

Monitorizar servidor tiene una gran selección de beneficios para las empresas; permite optimizar la instalación y los componentes de la misma, así como anticipar cualquier tipo de problema como caída del servidor.

- Existen plataformas permite monitorizar nada más y nada menos que 10.000 nodos, y cubre sin ningún tipo de limitación la monitorización de redes. Se integra de maravilla con los dispositivos móviles.
- Existen plataformas permite monitorizar servidores a través de un panel de control personalizable que presenta una gran flexibilidad.

  Tanto los servidores Cloud como los VPS de Axarnet están 100% administrados y cuentan con soporte técnico de la mano de grandes profesionales las 24 horas del

día los 7 días de la semana. Un amplio abanico de planes de diferentes precios que se adaptan a todo tipo de necesidades y preferencias.

b) Un error de código.

El código de error 500 es uno de los más comunes es el que nos muestra y ofrece el servidor cuando falla al completar una solicitud o petición que en principio parece correcta.
Cuando se le realiza una solicitud al servidor y esta falla antes de servirla, puede deberse a varios motivos, no uno sólo. Por ello podremos encontrar diferentes códigos de error 500 que nos identificarán los distintos tipos de motivos por los que se han producido y por los que no se ha completado la petición.
Englobamos todos con el formato numérico 5xx, es decir de la centena de 500, empiezan por tanto por el 5 seguido de dos cifras las cuales indicarán que tipo de error da imposibilidad de completar una petición.

c) Un ataque informático por parte hacker.

Para estar preparados para ataque de ciberseguridad siempre se debe tener en cuenta las siguientes pautas:

- Definir una **política de seguridad y buenas prácticas** para evitar la fuga o el robo de información.
- Crear un sistema de clasificación de la información
- **Definir roles y niveles de acceso a la información** dentro de la empresa
- Implementar un monitoreo en red ya que permite conocer en tiempo real el estado de los sistemas.
- Rastrear las IP sospechosas que hacen intentos seguidos por violar la seguridad y a partir de esto bloquearlas para evitar inconvenientes con el sitio web.

Gestión y monitoreo.

una vez que se tiene listo el plan de contingencia, es importante monitorear los sitios, que estos no tengan intentos de ataques cibernéticos y que estén en constante funcionamiento los enlaces funcionando, que el sitio no presente ningún problema en escritorio ni para móvil, buen tiempo de carga para todos los dominios estos tiempos de carga se pueden revisar en el dominio pagespeed.

Aprendizajes.

Se documenta la experiencia de la crisis, los aciertos, los errores, el impacto y las oportunidades, con el fin de hacer un seguimiento y un control a posibles crisis que se puedan presentar en los sitios o en los dominios bajo la administración del equipo web master Uniremington.

Desafíos

Entre los riesgos que se identificaron y pueden generar una crisis para Uniremington, se encuentran:

- Pronunciamientos negativos o que impacten a Uniremington directamente o indirectamente.
- Quejas y reclamos de parte de nuestra comunidad, inconforme con publicaciones de noticias o eventos realizadas por nuestro equipo.
- Cometarios, críticas fuertes y directas a directivos de Uniremington, como, por ejemplo, al rector, un docente o personal administrativo.

Claves para manejar una crisis apropiadamente.

Para atender una crisis de los sitios web se debe tener en cuenta las siguientes pautas o pasos los cuales nos ayudaran a levantar nuestros sitios lo más pronto posible.

- Se debe tener presente que siempre se tiene un backup de respaldo el cual se realiza cada mes guardando una copia de los cambios realizados en el último periodo con este se puede restaurar el sitio lo más pronto posible.

- Siempre empezar revisando si el causante de la caída del sitio no es por parte de la empresa. la cual presta el servicio de hosting y dominio en caso de que esta sea el causante comunicarse de inmediato con la empresa proveedora del servicio la cual nos proveerá las pautas para la restauración de nuestro sitio.
- Es importante tener claro el público que nos visita y cuál es su percepción con respecto a la gestión que realizamos. Esto nos ayudara a comprender las necesidades de los usuarios y hacer las correcciones pertinentes para el beneficio de la comunidad.

Destinatarios del protocolo.

Este protocolo es un documento de consulta para todas las personas que tengan relación directa o indirecta con el manejo de los Sitios web de Uniremington, quienes pueden ser: Web master, Auxiliar web master o cualquier persona que esté relacionada con este tema.

La caída de los sitios web es una situación común esto puede ocasionarse por diferentes factores como: un error del servidor, en el hosting, dominio etc. para esta situación siempre se debe estar preparado, en nuestro caso poseemos con un backup del sitio en su última versión, el cual se realiza este respaldo una vez al mes también, poseemos plugins de seguridad instalados en los sitios web para evitar el ataque de posibles hackers o aplicaciones con malas intenciones que puedan afectar nuestros sitios web.

se cuenta con el apoyo de la agencia de desarrollo web creativa para cualquier inconveniente que no se pueda resolver directamente desde las direcciones internas de la universidad.

CONTROL DE CAMBIOS

N°.	VERSIÓN INICIAL	BREVE DESCRIPCIÓN DEL CAMBIO	VERSIÓN FINAL	FECHA
1	**-**	Creación del documento	**01**	**23/04/2020**

ELABORÓ:	REVISÓ:	APROBÓ:
Analista Web Master	Director de Mercadeo	Director de Mercadeo
Fecha: 13/03/2020	**Fecha: 17/04/2020**	**Fecha: 23/04/2020**