MANUAL DE CONTROL DE ACCESO Y RESPALDOS DIARIOS DE LOS SITIOS WEB DE LAS GOBERNACIONES Y MUNICIPIOS

una ciudadanía ACTIVA para una mayor TRANSPARENCIA

Una iniciativa de:

GIAI Grupo Impulsor de Acceso a la información pública

Con el apoyo de:

UNIÓN EUROPEA

MANUAL DE CONTROL DE ACCESO Y RESPALDOS DIARIOS DE LOS SITIOS WEB DE LAS GOBERNACIONES Y MUNICIPIOS

Una iniciativa de:

GIAI Grupo Impulsor de Acceso a la información Pública

Con el apoyo de:

UNIÓN EUROPEA

Forman parte del GIAI

CEJ CENTRO DE ESTUDIOS JUDICIALES

Semillas para la Democracia

IDEA

libre FUNDACION

Ficha técnica

“Manual de control de acceso y respaldos diarios de los sitios web de las gobernaciones y municipios” es una publicación realizada por el Centro de Estudios Judiciales en el marco del Proyecto “Una ciudadanía activa para una mayor transparencia”, implementado por el Grupo Impulsor de Acceso a la Información Pública (GIAI) y cuenta con el apoyo de la Unión Europea (UE).

Centro de Estudios Judiciales, 2019.
Willian Richarson Nº 181 c/ calle Sajonia.
Asunción, C.P. 1645
Paraguay
www.cej.org.py
Contacto: cej@cej.org.py

ÍNDICE

Lista de Figuras 5

Acrónimos 6

1. Introducción 7

2. Objetivos 8

3. Perfiles de Usuarios y Contraseñas 9

4. Políticas de Respaldo y Recuperación de Datos 14

5. Formato de Sobres 18

Anexos. 21
I. Modelo Ficha de Envío de Respaldos
II. Modelo Ficha de Control de Respaldos

Referencias 23

LISTA DE FIGURAS

Figura 1. Proceso de Gestión de Contraseñas 7

Figura 2. Complementos para la administración de sitios web 8

Figura 3. Envío de Respaldo 10

Figura 4. Parte de atrás de envío de sobre de contraseña 11

Figura 5. Parte de atrás de envío de sobre de respaldo de datos 11

ACRÓNIMOS

CD	Compact Disc
CMS	Content Management System
DVD	Digital Versatile Disc
MITIC	Ministerio de Tecnologías de la Información y Comunicación
SMS	Short Message Service
IEC	International Electrotechnical Commission
ISO	International Organization for Standarization

1. INTRODUCCIÓN

La relevancia de los sitios web de las gobernaciones y los municipios en la actualidad, que además de ser sitios informativos de las actividades propias de cada gobernación o municipio, presentan información de interés público regulado por la Ley N° 5189/14, "Que establece la obligatoriedad de la provisión de informaciones en el uso de los recursos públicos sobre remuneraciones y otras retribuciones asignadas al servidor público de la República del Paraguay", y más recientemente la Ley N° 5282/14, "De libre acceso ciudadano a la información pública y transparencia gubernamental".

Ante la problemática que surge con el tratamiento de la información sensible de los sitios web asociados a las gobernaciones y municipios, debido a la pérdida de los niveles de acceso en cambios de gobierno o pérdida de datos por falta de procedimientos estandarizados producto de factores externos que atentan contra la integridad, disponibilidad y confidencialidad de los sitios web publicados, surge la necesidad de establecer procedimientos que estandaricen y aseguren un correcto tratamiento ante incidentes o cambios de gobierno.

Toda la información expuesta por las gobernaciones debería estar siempre disponible y actualizada. En el cambio de cada gobierno se debe asegurar que la información se encuentre accesible ya sea a nivel público, como a nivel administrativo para dar continuidad a los trabajos realizados en las gobernaciones anteriores.

El presente documento busca establecer un manual para el tratamiento de los niveles de acceso a los sitios web de las gobernaciones y municipios, así como, establecer los procedimientos necesarios para asegurar los respaldos de los trabajos realizados en cada sitio web, y la disponibilidad de los mismos ante la caída ya sea producto de alguna intrusión o problemas de los servidores físicos que hospedan los sitios actuales.

2. OBJETIVOS

1

Elaborar un manual para el tratamiento de los accesos a los sitios web de las gobernaciones y municipios.

2

Establecer los procedimientos necesarios para asegurar los respaldos de los trabajos realizados en cada sitio web, y la disponibilidad de los mismos ante la caída ya sea producto de alguna intrusión o problemas de los servidores físicos que hospedan los sitios actuales.

3. PERFILES DE USUARIOS Y CONTRASEÑAS

Los sitios web se han vuelto una de las herramientas de uso más frecuente para transmitir información de interés a un público determinado, así como de interacción con el mismo. Dado el valor de los contenidos que se publican en los sitios web, custodiar la información albergada en los mismos, se ha vuelto una tarea cada vez más relevante, buscando sostener siempre la integridad, confidencialidad y disponibilidad de la información.

Para gerenciar adecuadamente cualquier servicio informático, es importante hacer uso de perfiles de gestión y administración, entendiendo los roles de cada uno y su valor en el sostenimiento del servicio. Básicamente, los perfiles son los que logran establecer el flujo de trabajo de la organización, en relación con las publicaciones y su administración.

Pueden existir diferentes tipos de perfiles asociados a los sitios web, cambiando dichos perfiles acorde a las características o funcionalidades propias de los sistemas de gestión de contenidos (en adelante CMS, por sus siglas en inglés) existentes en el mercado como Wordpress[1], Joomla[2], Drupal[3], Modx[4] entre otros o de CMS desarrollados a medida por empresas de desarrollo. Nosotros describimos a continuación los tres perfiles principales de usuario, con los cuales deberían contar los CMS.

[1] https://es.wordpress.com/
[2] https://www.joomla.org
[3] https://www.drupal.org
[4] https://modx.com

1. Perfil Suscriptor

Es un perfil básico, que no tiene capacidades relacionadas a la gestión de contenidos, pero suele ser utilizado cuando el sitio web administrado permite interacción con los usuarios o internautas. Entonces, mediante un registo básico, los usuarios de este perfil pueden dejar comentarios en el sitio web, además la existencia de este perfil le permite al administrador del sitio, direccionar visualizaciones de ciertos contenidos a grupos específicos de suscriptores.

2. Perfil Editor

El perfil editor tiene acceso a todo el contenido del sitio pudiéndo modificarlo según necesidad, algunos CMS separan el perfil editor del perfil autor, pero en cualquiera de los casos, este perfil no debería tiene capacidad de administración fuera de los contenidos, es decir, no puede gestionar usuarios, temas, *plugins*, menús, *widgets* entre otros.

3. Perfil Administrador

El perfil administrador tiene acceso a toda la plataforma del sitio, ya sea acceso a todos los elementos del escritorio que constituyen al sistema manejador de contenidos, a la administración de los usuarios de la plataforma, a los temas que el CMS permite utilizar, plugins y cualquier contenido asociado al sitio.

El usuario administrador es el más crítico dentro de la plataforma CMS. Una vez que el sitio se encuentra funcional no debería ser necesario en la operativa cotidiana el usuario administrador. Para asegurar una continuidad en el tiempo de los desarrollos del sitio, y por las características del usuario administrador, la contraseña del mismo debería ser resguardada bajo llave. Para el resguardo de la contraseña del administrador, establecemos el siguiente procedimiento:

1. Se deben seleccionar dos personas críticas dentro de la institución que serán los encargados de generar la contraseña.
2. Cada persona generará la mitad de la contraseña, sin compartirla con nadie (ni siquiera entre ellos). Pero este proceso significa que debe ser ejecutado al mismo tiempo por ambas personas. Los criterios para establecer una contraseña segura serán descriptos más abajo dentro de esta sección.
3. Cada mitad de contraseña será escrita en un papel con letra legible, para que luego ambos papeles sean guardados en un sobre lacrado.
4. El sobre lacrado deberá ser remitido a una segunda parte neutral, que en este caso puede ser considerado el MITIC como un punto focal objetivo. El MITIC en este caso debe guardar la contraseña en un lugar lo suficientemente seguro, como una caja fuerte o el lugar que se considere pertinente.
5. En caso, que la gobernación o municipio requiriese de esta contraseña la misma debe ser solicitada por nota, para cuyo caso el firmante de la nota debe ser una persona adecuadamente identificada por el MITIC como responsable dentro de la gobernación o municipio. Una vez abierto el sobre, se deberá volver a realizar una nueva contraseña, repitiendo el procedimiento anteriormente explicado.

El lugar seleccionado como parte neutral (en este caso MITIC), debe contar con las condiciones físicas, ambientales y de seguridad para guardar las contraseñas; así como debe contar con personal adecuado para atender los casos de todos los municipios y gobernaciones.

A su vez, si hubiese algún atentado o sospecha de atentado contra la privacidad del sitio, la contraseña del administrador debe ser modificada y debe volver a realizarse el procedimiento anteriormente descripto. Las etapas descriptas pueden visualizarce en la Figura 1.

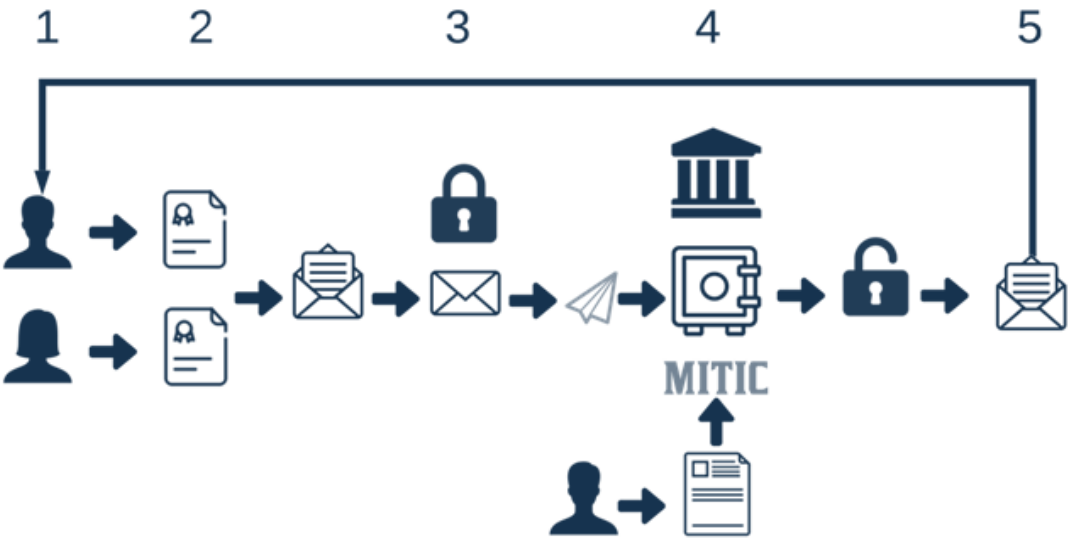

Figura 1. Procedimiento de gestión de contraseña administrador.

Si bien, este procedimiento está pensado para los sitios web, también puede ser utilizado para cualquiera de los servidores con que cuente bajo su administración la gobernación o municipio.

Para establecer contraseñas seguras, en cualquiera de los servicios ofrecidos dentro de una institución, se deben tener presente algunos criterios básicos como:

- evitar palabras del diccionario, nombres, números;
- evitar palabras en idiomas comunes;
- combinar letras con números y caracteres especiales;
- establecer longitudes de las contraseñas de al menos 15 caracteres; así como,
- las contraseñas de usuario que tienen perfiles de gestión cotidiana, deberían ser cambiadas al menos cada seis meses o según se considere pertinente o a la finalización del año fiscal.

Cabe mencionar, que alguno de los complementos (ver Figura 2) necesarios para la administración de cualquier servicio de acceso remoto con que cuente la institución deben considerar:

- Uso de certificados, en particular para el acceso a los servicios web.
- Uso de captcha, siempre que el sitio web requiera de interacción con el usuario.
- Sistemas de Doble autenticación, ya sea mediante la utilización de doble contraseña o mediante la validación de pin obtenido vía SMS o correo electrónico.

Figura 2. Complementos para la administración de sitios web.

4. POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE DATOS

En esta sección, se busca establecer las directrices para el proceso de respaldo de datos, así como las consideraciones a tener presente para la recuperación de datos después de una eventual falla, ya sea falla de *hardware* o falla de *software*, que produzca una pérdida de información.

La norma ISO/IEC 27.002:2013, da las indicaciones necesarias para realizar copias de respaldo de la información y del software, considerando los siguientes elementos:

a) es recomendable definir el nivel necesario para establecer la información de respaldo;

b) se deberían hacer registros exactos y completos de las copias de respaldo y generar procedimientos de restauración;

c) la extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos deberían reflejar las necesidades de la organización, los requisitos de seguridad de la información involucrada y la importancia de la operación continua de la organización;

d) los respaldos *(backup)* se deberían almacenar en un sitio lejano, a una distancia suficiente para escapar a cualquier daño debido a desastres y/o catástrofes naturales en la sede principal;

e) a la información de respaldo se le debería dar un grado apropiado de protección física y ambiental coincidente con las normas aplicadas en la sede principal;

f) es conveniente probar con regularidad los medios de respaldo para garantizar que sean confiables para uso en emergencias, cuando sea necesario;

g) los procedimientos de restauración se deberían verificar y probar con regularidad para garantizar su eficiencia y que se puedan completar dentro del tiempo designado en los procedimientos operativos para la recuperación;

h) en situaciones en donde es importante la confidencialidad, los respaldos se deberían proteger por medio de encriptación.

Para sistemas críticos, las disposiciones de respaldo deberían comprender toda la información de los sistemas, las aplicaciones y los datos necesarios para recuperar todo el sistema en caso de desastre.

A partir de los puntos citados establecemos algunas directrices puntuales recomendadas para el proceso de *backups* [2]:

- la información considerada crítica de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento externo como dispositivos ópticos, como CD o DVD, disco duro externo, etc;
- el departamento de informática, debe establecer un calendario de la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación) que se deben aplicar sobre la información respaldada;
- todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso reservado solamente a personas autorizadas por el área del departamento de informática;
- las copias de respaldo se guardarán con el objetivo de restaurar o recuperar datos luego de un virus informático que corrompa la información, defectos en los discos de almacenamiento, problemas con los servidores o computadores, materialización de amenazas, catástrofes naturales y por requerimiento legal;
- la restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información;
- semanalmente o según nivel de actualización de la información, el departamento de informática, verificará la correcta ejecución de los procesos de backup, y suministrará los medios de almacenamiento requeridos para cada trabajo;
- el backup debe cubrir aplicaciones y base de datos;
- el departamento de informática debe mantener un inventario actualizado de las copias de respaldo de la información, los aplicativos y/o sistemas; y
- los medios de almacenamiento que vayan a ser eliminados deben pasar un proceso de borrado seguro y posteriormente el medio debe ser eliminado o destruido de forma adecuada. El borrado seguro es un proceso de formateo a bajo nivel, donde se escriben ceros en la superficie lógica de almacenamiento, no permitiendo que la referida información se pueda recuperar posteriormente.

Una vez realizado un backup, el mismo debe ser remitido a un lugar externo (ver Figura 3), para su resguardo, al menos, cada cierta frecuencia de tiempo dependiendo el dinamismo de actualización de la información que estoy respaldando. En este sentido, se debe considerar al MITIC como un lugar objetivo de almacenamiento de los respaldos por gobernación y/o municipio, resguardando todos los procedimientos necesarios para asegurar la confidencialidad respectiva de la información que se les confía. En el anexo I, se puede visualizar un modelo de ficha para el envío de respaldos, mientras que en el anexo II, se puede visualizar un modelo de ficha para llevar un control por parte del área técnica de la gobernación o municipio de la integridad de los respaldos que se van realizando.

Figura 3. Envío de Respaldo.

El lugar externo, debe contar con las condiciones físicas, ambientales y de seguridad para guardar los respaldos; así como debe contar con personal adecuado para atender los casos de todos los municipios y gobernaciones.

5. FORMATO DE SOBRES

Más arriba, se menciona el envío de información a un ente externo en un sobre lacrado para dos casos particulares, siendo de suma relevancia uniformizar el criterio para todas las gobernaciones y municipios, para una mejor gestión del receptor de los sobres.

▪ Sobre de Envío de Contraseñas

La parte de atrás del sobre debe contener en el vértice superior izquierdo el logo de la gobernación o municipio y en el vértice superior derecho en un formato Times New Roman de tamaño 32 el número de secuencia de sobre que está siendo remitido y el año de remisión. A modo de ejemplo, el número del sobre quedaría en NúmeroSecuencia/Año. El número de secuencia debería ser reiniciado cada año.

En el centro del sobre en un formato Times New Roman de tamaño 28 debe contener el nombre de la gobernación o municipio y en la línea de abajo debe decir “RESPALDO DE DATOS”, así como las palabras “SITIOS WEB”.

En el frente del sobre, debe contener el nombre de la gobernación o municipio y la palabra “CONFIDENCIAL”.

En la Figura 4, se puede visualizar un modelo de como debería de quedar el sobre en la parte de atrás.

Figura 4. Parte de atrás de sobre de envío de contraseñas.

▪ Sobre de Envío de *Backup*

La parte de atrás del sobre debe contener en el vértice superior izquierdo el logo de la gobernación o municipio y en el vértice superior derecho en un formato Times New Roman de tamaño 32 el número de secuencia de sobre que está siendo remitido y el año de remisión. A modo de ejemplo, el número del sobre quedaría en NúmeroSecuencia/Año. El número de secuencia debería ser reiniciado cada año.

En el centro del sobre en un formato Times New Roman de tamaño 28 debe contener el nombre de la gobernación o municipio y en la línea de abajo debe decir “RESPALDO DE DATOS”, así como las palabras “SITIOS WEB”.

En el frente del sobre, debe contener el nombre de la gobernación o municipio y la palabra “CONFIDENCIAL”.

En la Figura 5, se puede visualizar un modelo de como debería de quedar el sobre en la parte de atrás.

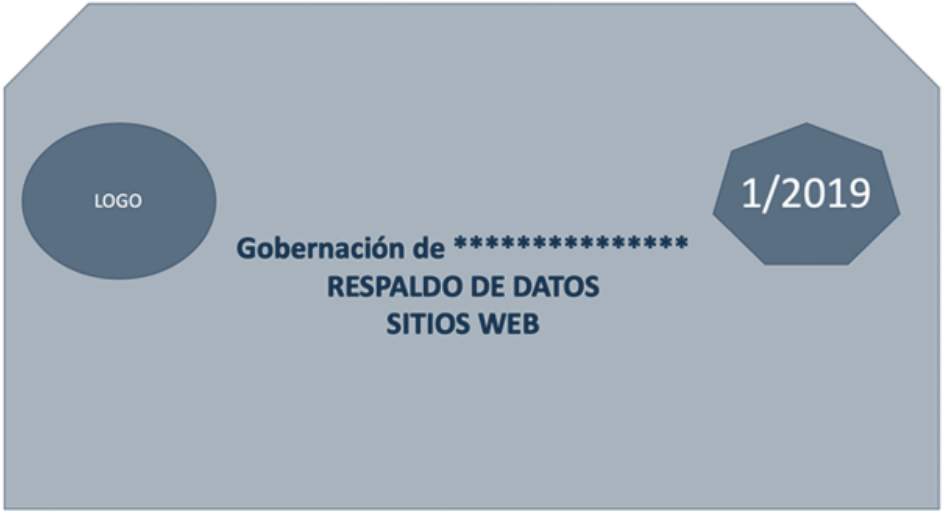

Figura 5. Parte de atrás de sobre de envío de respaldo de datos.

ANEXOS

I. Modelo Ficha de Envío de Respaldos

LOGO

Ficha de Envío de Respaldos

Fecha envio	Contenido del Backup	Fecha Backup	Responsable de Envío	Firma	Responsable Transporte	Firma	Destino

II. Modelo Ficha de Control de Respaldos

Fecha Prueba	Contenido del Backup	Fecha Backup	Aprobado (SI/NO)	Responsable Prueba	Firma

REFERENCIAS

- BSI Group. ISO 22301 Gestión de la Continuidad de Negocio.
- https://www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/
- MANUAL DE LA POLÍTICA DE SEGURIDAD PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - TICS. Presidencia de la República de Colombia. Mayo, 2016. http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Sistema-Seguridad-Informacion.pdf
- http://iso27000.es/iso27002.html

www.giai.org.py

 GIAI_Py

 @GIAI_Py