



MANUAL DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

TABLA DE CONTENIDO:

1. INTRODUCCIÓN
2. OBJETIVOS
3. ALCANCES
4. DEFINICIONES
5. POLÍTICAS GENERALES DE SEGURIDAD FISICA
6. POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS (TRABAJADORES Y DIRECTIVOS)
7. POLITICAS ORIENTADAS A LOS USUARIOS EXTERNOS (ASOCIADOS/WI-FI)
8. POLÍTICAS DE ADMINISTRACIÓN DE LOS BACKUPS
9. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB
10. POLÍTICAS DE MANEJO Y ADMINISTRACIÓN DE LAS REDES SOCIALES CORPORATIVAS
11. CUMPLIMIENTO DE LAS POLITICAS DE SEGURIDAD INFORMÁTICA.



1.- INTRODUCCIÓN

Con los avances de la Informática y el Internet y las Telecomunicaciones, la Seguridad Informática es una prioridad dentro de las organizaciones modernas, y es necesaria para:

- Protección,
- Mantenimiento,
- Control de Acceso,
- Confidencialidad,
- Integridad y
- Disponibilidad de la información.

Las Políticas de Seguridad Informática son las directrices de índole técnica y organizacional que deben seguirse a fin de proteger y resguardar tanto el funcionamiento como la información contenida en los sistemas de información. Siendo la información institucional, un activo valioso para ACENESPAR, se hace necesario no sólo la implementación de herramientas de hardware y software de seguridad, llevadas a cabo por terceros (OPTICAL NETWORKS – “FORTINET” y SECURITY LABS- “ESET ANTIVIRUS”) sino involucrar a todo el personal para proteger la integridad y confidencialidad de los datos.

Las Políticas de Seguridad Informática, en adelante llamadas simplemente PSI, deben ser aplicadas y acatadas por todo el personal de ACENESPAR, incluidos personal operativo, administrativo y jerárquico.

Este manual, tiene como finalidad dar a conocer las PSI, entendiendo como premisa que la seguridad de la información es responsabilidad y tarea de todos.



2.- OBJETIVOS

- a) Definir e implementar las políticas de Seguridad Informática(PSI) que dan las pautas y rigen la gestión, el uso adecuado y la seguridad de la información de los sistemas informáticos y en general de todo el parque informático (hardware como computadoras, monitores, impresoras, scanners, parlantes, antenas WiFi, anexos VoIP, etc. y el software tanto el software base –Windows- como los aplicativos – Office- y sistemas como el ORION para los restaurantes, bar y cafetería, el SISCONT para Contabilidad y Tesorería, el GESTORPLUS para el área de Bienes Patrimoniales, el SISTEMA DE ASISTENCIA para el área de RRHH, el SISTEMA DE ASOCIADOS para el control de Ingreso de Asociados y control del pago de cuotas de mantenimiento y el nuevo SISTEMA INTEGRAL en desarrollo.
- b) Las políticas de Seguridad Informática, deben definirse bajo 2 aspectos básicos, pero sumamente importantes:
 - 1. Lo que hay que hacer o fomentar.
 - 2. Lo que debemos evitar.
- c) Estos lineamientos que se planteen, deben ser interiorizados, aplicados y verificados permanentemente.



3.- ALCANCES

Tal como se mencionó en la parte introductoria de este manual, las PSI están orientadas a salvaguardar toda la información almacenada, procesada y transmitida por medios electrónicos.

Estas PSI deben ser conocidas, difundidas y cumplidas tanto por el personal operativo, administrativo y jerárquico que cumplan una labor o gestión a través de algún dispositivo computarizado o electrónico dentro de las instalaciones de las diferentes Sedes de ACENESPAR, llámense Sede Principal, de Ciudad o Camacho, Sede de Campo o de Ñaña, Sede de Playa o de Curayacu, Sede Educativa o Colegio HPC y las Villas de Cusco y Tumbes.

4.- DEFINICIONES

Para entender el presente Manual de PSI, se adoptarán las siguientes definiciones:

- 1) **Acceso físico:** Es la posibilidad de acceder físicamente a un computador o dispositivo, manipularlo tanto interna como externamente.
- 2) **Acceso lógico:** Ingresar al sistema operativo o aplicaciones de los equipos y manipularlos, ya sea directamente, a través de la red local o por Internet.
- 3) **Activos de Información:** Toda aquella información que la Asociación considera importante o fundamental para sus procesos, como documentos, bases de datos, contratos, acuerdos, documentación de los sistemas, manuales de usuarios, aplicaciones, software de los sistemas, etc.
- 4) **Aplicaciones o aplicativos:** Son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadoras, tablets o celulares.



- 5) **Cableado estructurado:** Cableado de un edificio o serie de edificios que permiten interconectar equipos activos, de diferente o igual tecnología permitiendo la integración de los diferentes servicios que dependen de las interconexiones físicas como datos, telefonía, control, etc.
- 6) **Cifrado de datos:** Proceso por el que una información legible se transforma mediante un algoritmo llamado cifra, en información ilegible llamada criptograma o secreto. Esta información ilegible sólo se vuelve legible a través de la cifra. Si se dispone de dicha cifra puede ser leída y retransmitida sin riesgo de terceras partes.
- 7) **Configuración lógica:** Conjunto de datos que determina el valor de algunas variables de un programa o de un sistema y elegir entre distintas opciones para obtener un programa o sistema personalizado o para que pueda funcionar correctamente.
- 8) **Copia de respaldo o Backup:** Operación que consiste en duplicar y asegurar datos e información contenida en uno o varios sistemas informáticos. Es la copia de seguridad.
- 9) **Contenido:** Todos los tipos de información o datos que se manejan a través de los diversos servicios informáticos, como textos, imágenes, video, diseños, software, animaciones, etc.
- 10) **Contraseñas:** Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos
- 11) **Cuenta de Correo Institucional:** Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos, que se encuentran alojados en un hosting de propiedad o alquilado por la Asociación.
- 12) **Cuenta de Acceso:** Colección de información que permite a un usuario identificarse en un sistema informático o servicio, mediante un usuario y una contraseña, para tener acceso al sistema y operar dentro de él.
- 13) **Dispositivos Periféricos:** Aparatos auxiliares e independientes conectados al computador o a la red local.



- 14) Dominio:** Es un conjunto de computadoras, conectadas en una red, que confían a uno de los equipos de dicha red, normalmente un servidor, la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red.
- 15) Espacio en disco duro:** Capacidad de almacenamiento de datos en una unidad de disco duro.
- 16) Herramientas ofimáticas:** Conjunto de aplicaciones informáticas que se utilizan en funciones de oficina para optimizar, automatizar y mejorar los procedimientos o tareas relacionadas. En la Institución se hace uso de la herramienta Microsoft Office en sus versiones 2010, 2013 y 2016 pero no licenciadas.
- 17) Información confidencial:** Se trata de una propiedad de la información que pretende garantizar el acceso sólo a personas autorizadas.
- 18) Información/Documento electrónico:** Es la información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares. Se clasifican por su forma o formato en documentos ofimáticos, cartográficos, correos electrónicos, imágenes, videos, audio, mensajes de datos de redes sociales, formularios electrónicos, bases de datos, etc.
- 19) Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información.
- 20) Licencia de uso:** Contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatarario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas, es decir, es un conjunto de permisos que un desarrollador le puede otorgar a un usuario en los que tiene la posibilidad de distribuir, usar y/o modificar el producto bajo una licencia determinada.



- 21) Mantenimiento lógico preventivo:** Es el trabajo realizado en el disco duro del equipo de cómputo, con la finalidad de mejorar el rendimiento general del sistema operativo.
- 22) Mantenimiento físico preventivo:** Actividad de limpieza de elementos como polvo, residuos de alimentos y otro tipo de partículas, que debe realizarse en el equipo de cómputo, con el propósito de posibilitar que su correcto funcionamiento sea más prolongado en el tiempo.
- 23) Medios de almacenamiento extraíble:** Son aquellos soportes de almacenamiento, diseñados para ser extraídos del computador sin tener que apagarlo. Por ejemplo, memorias USB, discos duros externos, discos ópticos (CD, DVD), tarjetas de memoria (SD, Compact Flash, Memory Stick).
- 24) Plataforma web:** Sistema que permite la ejecución de diversas aplicaciones bajo un mismo entorno, dando a los usuarios la posibilidad de acceder a ellas a través de internet.
- 25) Propiedad intelectual:** Se relaciona con las creaciones de la mente como invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizadas en el comercio. Es el conjunto de derechos que corresponden a los autores y a otros titulares.
- 26) Recurso Informático:** Todos aquellos componentes de hardware y programas o software que son necesarios para el buen funcionamiento de un computador o un sistema de gestión de la información. Incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.
- 27) Red de datos:** Es un conjunto de ordenadores que están conectados entre sí y comparten recursos, información y servicios.
- 28) Riesgo:** Posibilidad de que se produzca un contratiempo o una desgracia, las vulnerabilidades y amenazas a que se encuentran expuestos los activos de información.



- 29) Servicio Informático:** Conjunto de actividades asociadas al manejo automatizado de la información que satisfacen las necesidades de los usuarios.
- 30) Servidor:** Se entiende como el software que configura una PC como servidor para facilitar el acceso a la red y sus recursos. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los usuarios usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde están trabajando.
- 31) Sistema de Información:** Es un conjunto de elementos orientados al tratamiento y administración de los datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.
- 32) Software Antivirus:** Son programas que buscan prevenir, detectar y eliminar virus informáticos. En los últimos años, y debido a la expansión del Internet, nuevos navegadores y la ingeniería social, los antivirus han evolucionado para detectar software fraudulento conocido como malware.
- 33) Software de gestión:** Son aquellos programas utilizados a nivel empresarial, para emprender algo y que por su aplicación persigue fines lucrativos y no lucrativos. Es un software que permite gestionar todos los procesos de un negocio o una empresa en forma integrada.
- 34) Software malicioso:** Programas diseñados específicamente para dañar las computadoras, instala códigos de programa o virus sin consentimiento del usuario
- 35) Tráfico de red:** Es la cantidad de datos enviados y recibidos por los usuarios de la red.
- 36) UPS:** Sistema de alimentación ininterrumpida, dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, pueden proporcionar energía eléctrica por cierto tiempo a los dispositivos conectados a él, durante un apagón eléctrico.



5.- POLÍTICAS GENERALES DE SEGURIDAD FÍSICA

- a) Se debe destinar un área específica en la Asociación como DATA CENTER, donde se ubican los sistemas de Telecomunicaciones y los Servidores, debidamente protegidos con la infraestructura adecuada, de manera que se restrinja el acceso directo a personas o usuarios no autorizados.
- b) Este Data Center, deberá contar con un sistema de protección contra Incendios, control de temperatura o Aire Acondicionado permanente a una temperatura no superior a 22 grados centígrados y sistema eléctrico de respaldo o UPS.
- c) El sistema contra Incendios deberá incluir Extintores tipo C para equipo eléctrico.
- d) Los equipos que se albergan en el Data Center, como servidores, cableados, switches, modem, routers, gateways, y dispositivos de almacenamiento, deben estar protegidos y libres de amenazas como robo, incendio, inundaciones, humedad, agentes biológicos, explosiones, vandalismo y terrorismo.
- e) Se debe evitar que personal ajeno a la Institución, haga uso de los equipos informáticos, utilice USB para colocar o extraer información que sea parte de los **Activos de Información**.
- f) Asimismo, el personal de la Institución no debe prestar o alquilar o ceder en uso bienes, equipos o documentación que sean parte de los **Activos de Información** o de los **Recursos Informáticos** de la Institución, a terceras personas, empresas u otras instituciones salvo excepciones especificadas en algún contrato de alquiler o reserva aprobados por la Gerencia y/o Presidencia.



6.- POLÍTICAS ESPECÍFICAS ORIENTADAS A LOS USUARIOS INTERNOS

- a) Todo personal (trabajador o funcionario), usuario de equipos de cómputo, software de gestión, aplicativos, plataforma web y servicios informáticos, debe aceptar las condiciones de confidencialidad y de uso adecuado de los recursos informáticos, así como cumplir las directrices del presente Manual.
- b) Los funcionarios y trabajadores que cesen en sus funciones o haya culminado su vínculo laboral o contractual con ACENESPAR, deberán hacer entrega formal de los equipos asignados como celulares, laptops, tablets o equipos de cómputo, así como la TOTALIDAD de la información electrónica que se produjo y se recibió con motivo de sus funciones y actividades, como requisito para su liquidación y constancia de trabajo.
- c) Toda información recibida y producida en el ejercicio de las funciones y cumplimiento de obligaciones contractuales, que se encuentre almacenada en los equipos de cómputo asignados, pertenece a ACENESPAR y por tanto no se hará divulgación ni extracción de la misma sin previa autorización de los Directivos de ACENESPAR.
- d) El retiro de la información electrónica considerada CONFIDENCIAL sólo podrá hacerse con la autorización del Directivo competente.
- e) Ningún funcionario o trabajador podrá visualizar, copiar, alterar o destruir información que no esté bajo su responsabilidad.
- f) Todo contrato o convenio relacionado con servicios informáticos y/o acceso a información, debe contener una cláusula donde el contratista acepte el conocimiento de las PSI y acuerde mantener confidencialidad de la información a través de la suscripción de un acuerdo o compromiso de



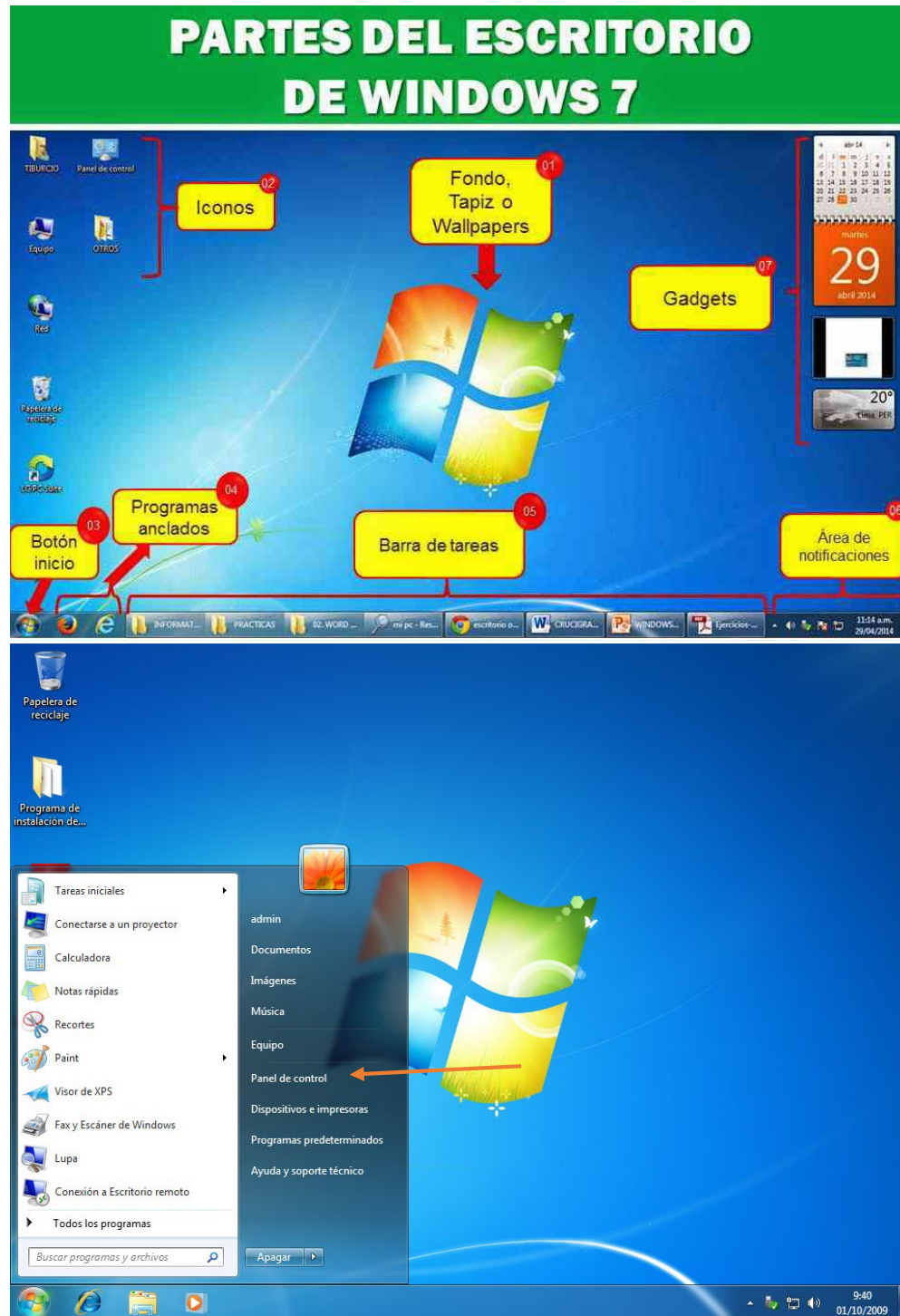
confidencialidad de la información y que debe hacerse extensivo a sus colaboradores.

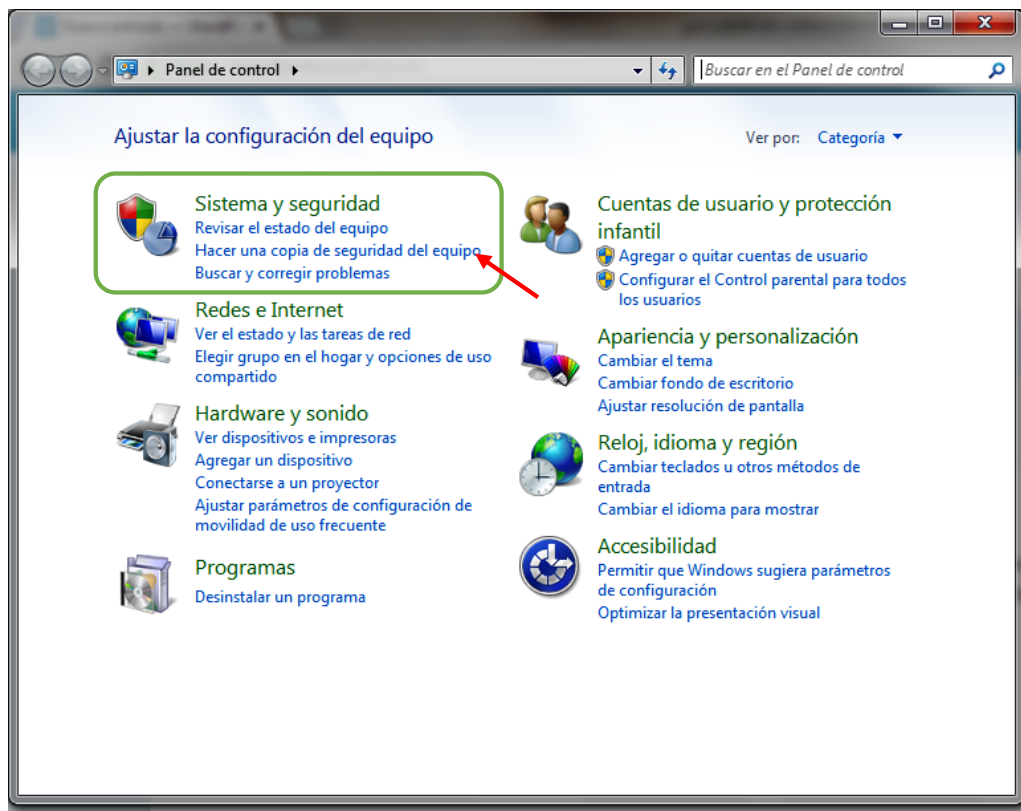
- g) La instalación y desinstalación de software, programas informáticos, configuración lógica, conexiones de red, instalación y desinstalación de dispositivos periféricos, manipulación interna y reubicación de equipos de cómputo y periféricos será realizada única y exclusivamente por personal del Área de Sistemas de ACENESPAR.
- h) El espacio en disco duro de los equipos de cómputo y Servidores pertenecientes a ACENESPAR, SERÁ OCUPADO ÚNICAMENTE CON INFORMACIÓN INSTITUCIONAL, no se hará uso de ellos para almacenar información personal como fotos, imágenes, documentos, música, video, etc.
- i) Los funcionarios y trabajadores que deban hacer uso de los recursos informáticos de la Institución, son responsables de tener conocimientos actualizados en informática básica y el uso de herramientas ofimática.
- j) Asimismo, los funcionarios y trabajadores serán responsables de llevar a cabo copias de seguridad de los datos y programas en forma periódica, que puede ser una vez cada día, al final de la jornada, una vez a la semana, al final de la semana o una vez al mes si el riesgo o volumen de la información no es alto.
- k) Para las actividades de copia de seguridad se ha asignado un disco externo de 2 TB a cada área.

Secretaria Presidencia	Dora Zevallos
Secretaria Gerencia	Margarita Rojas
Secretaria Gerencia Ciudad	Rosa Vargas
Asesoría Legal	Katia Jorge
Control de Asociados	Nataly Velarde
Tesorería	Flor Santos
RR.HH.	José Zapata
Contabilidad	José Calderón
Logística	Kymarina Perea
Almacén	Lenin Vilcapoma
Reservas y Contratos	Elizabeth Reyes

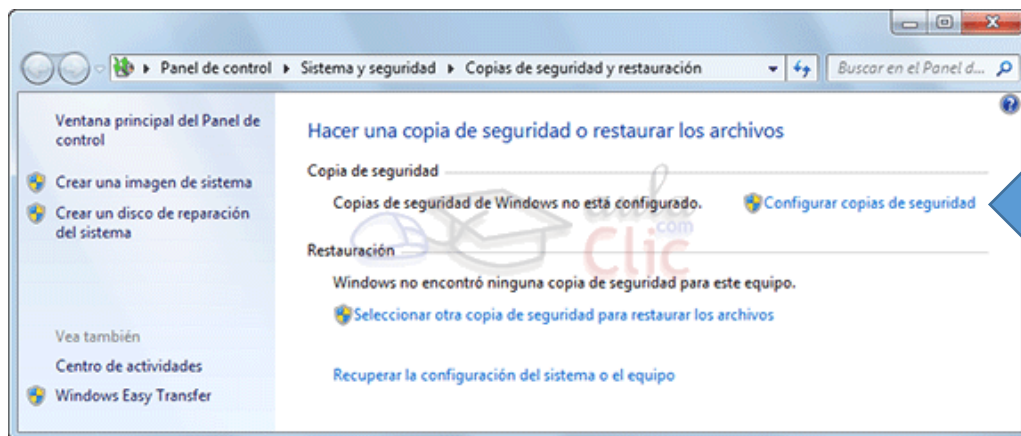
PROCEDIMIENTO DE BACKUP EN WINDOWS 7

Para iniciar la herramienta de Copia de Seguridad o Backup, tenemos que ir al botón de Inicio > Todos los programas > Panel de Control > Sistema y Seguridad > Copias de Seguridad y Restauración.

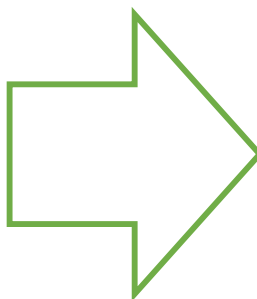


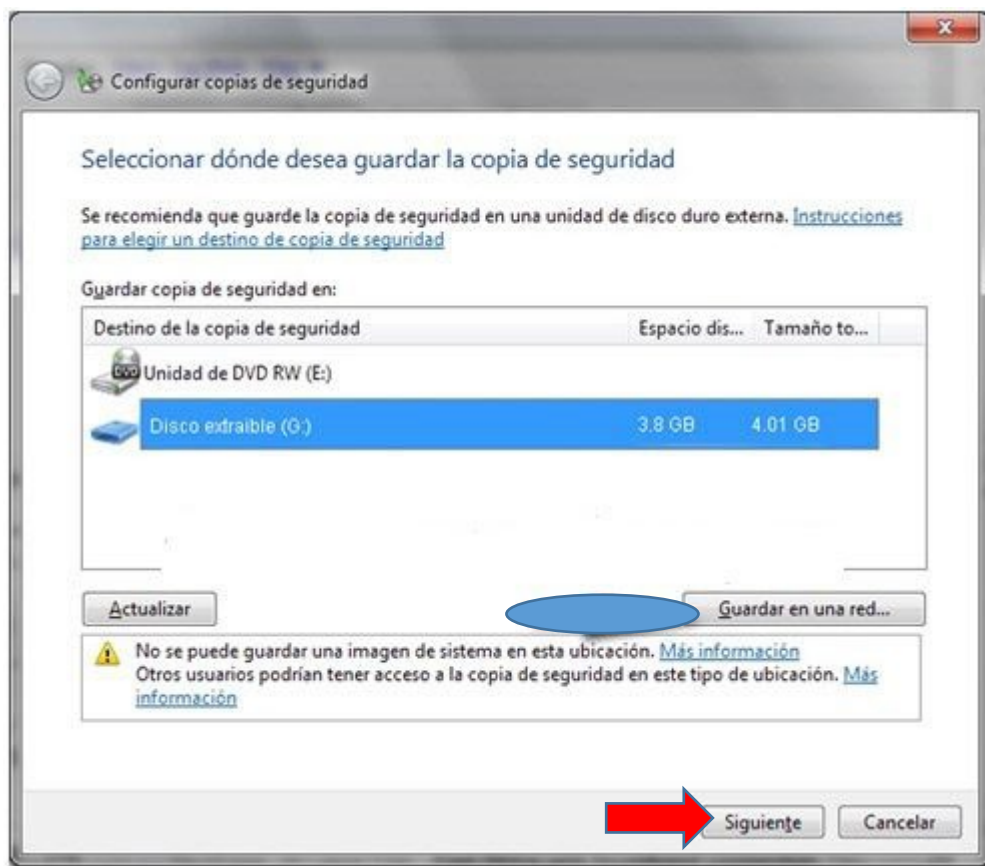


La primera vez que iniciamos esta herramienta, se verá la siguiente ventana:

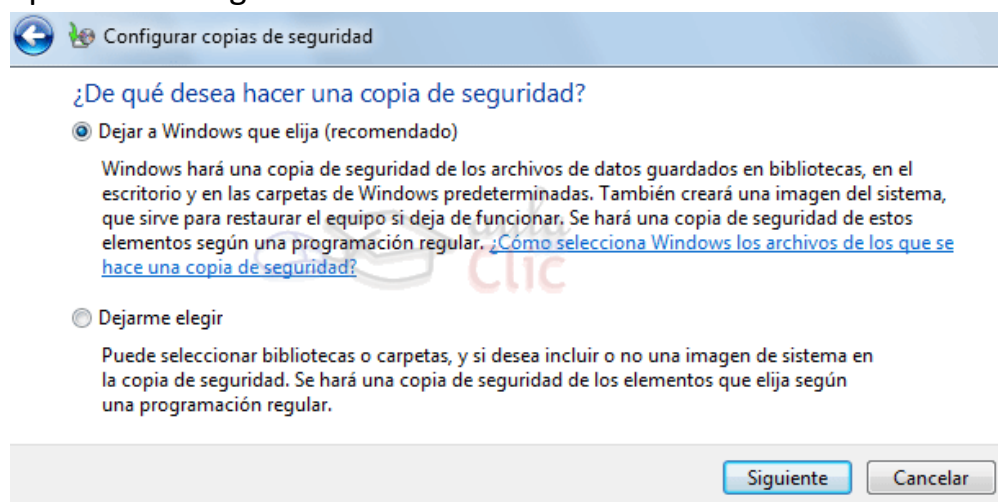


Hacemos clic donde dice “Configurar copias de seguridad”
Se abrirá una nueva ventana como la que se muestra más adelante:





Escogemos la que corresponde a nuestro disco duro externo que ya debe estar conectado al CPU vía cable USB. Luego hacemos clic en siguiente, y aparecerá la siguiente ventana



Si por error o por decisión propia, marcamos la segunda opción, veremos una ventana como la siguiente:



 Configurar copias de seguridad

¿De qué desea hacer una copia de seguridad?

Active la casilla de los elementos que desea incluir en la copia de seguridad. [¿Qué archivos se excluyen de forma predeterminada de la copia de seguridad?](#)

Archivos de datos

- ☐ Hacer copia de seguridad de los datos de usuarios recién creados
- ☒ Bibliotecas de aulaClic
- ☐ Bibliotecas de Melisa

Equipo

- ☐ HP (C:)
- ☐ Trabajo (K:)

☒ Incluir una imagen de sistema de las unidades: HP (C:), Trabajo (K:)

Una imagen de sistema es una copia de las unidades necesarias para que se ejecute Windows. Sirve para restaurar el equipo si deja de funcionar.

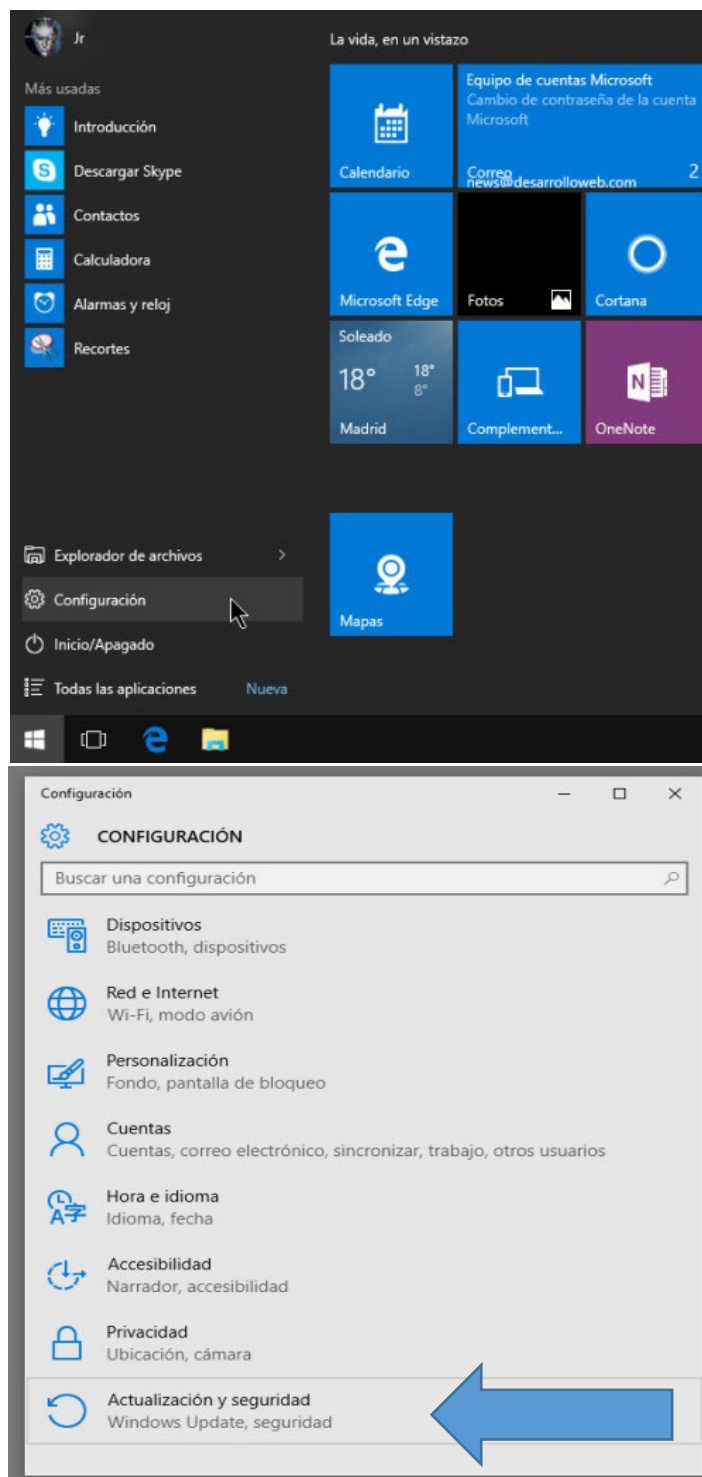
Podremos elegir qué bibliotecas de usuario nos interesa copiar e incluso qué contenido.

La otra opción es crear una imagen del sistema. Esta opción la realizará el personal del Área de Sistemas.



PROCEDIMIENTO DE BACKUP EN WINDOWS 10

Para iniciar la herramienta de Copia de Seguridad o Backup, tenemos que ir al botón de Windows> Configuración > Actualización y seguridad > Copia de Seguridad.





Configuración



Configuración de Windows

Buscar una opción de configuración



Sistema

Pantalla, sonido, notificaciones, energía



Dispositivos

Bluetooth, impresoras, mouse



Teléfono

Vincular Android o iPhone



Internet y red

Wi-Fi, modo de avión, VPN



Personalización

Fondo, pantalla de bloqueo, colores



Aplicaciones

Desinstalar, valores predeterminados, características opcionales



Cuentas

Tus cuentas, correo electrónico, opciones de sincronización, trabajo y familia



Hora e idioma

Voz, región, fecha



Juegos

Barra de juego, captura, difusión, modo de juego



Accesibilidad

Narrador, lupa, contraste alto



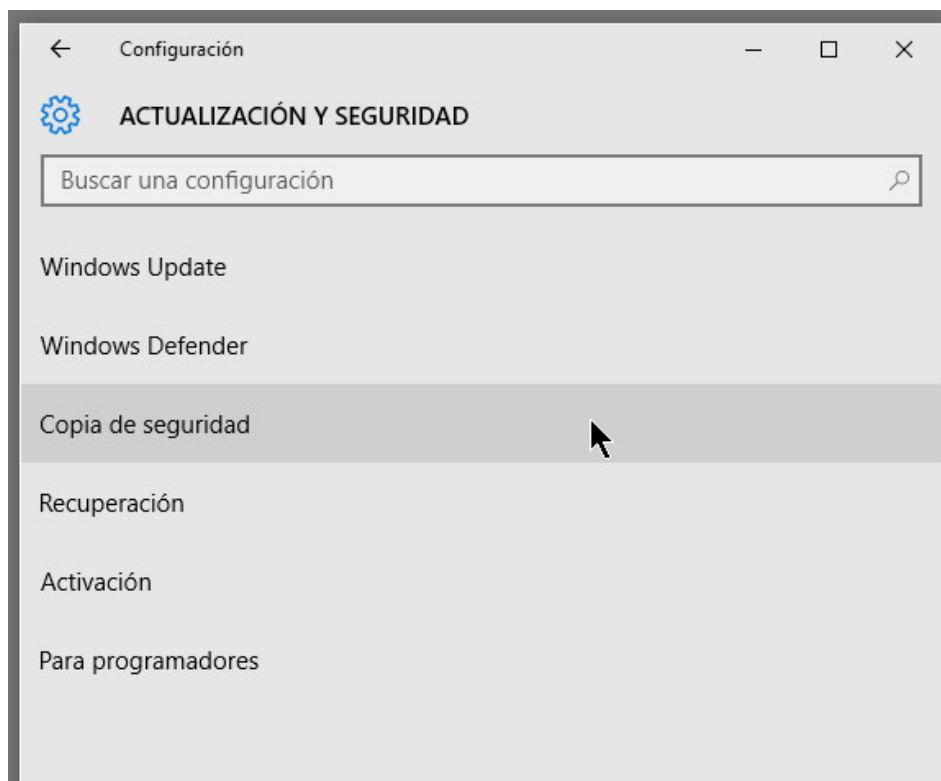
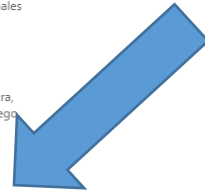
Privacidad

Ubicación, cámara



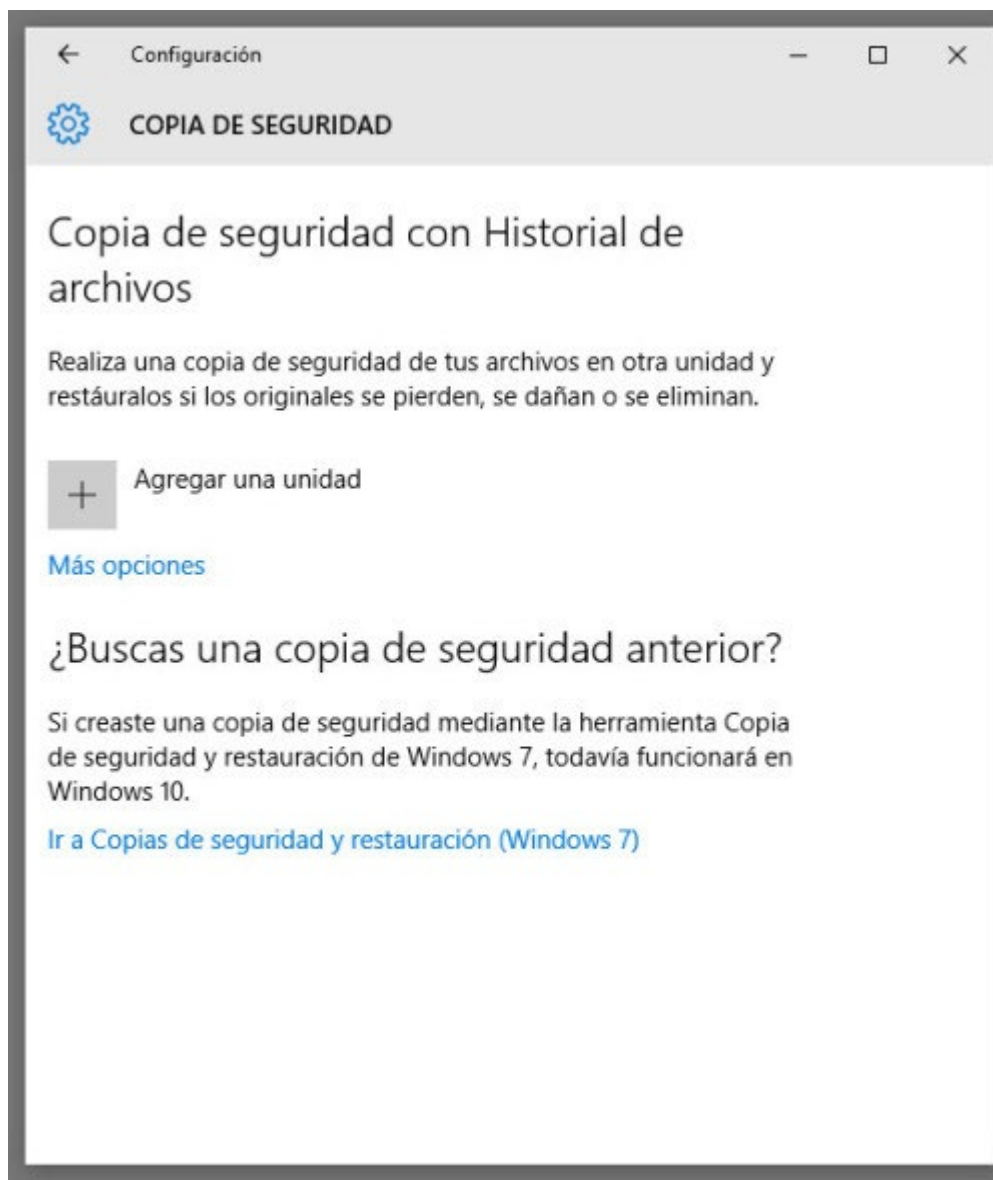
Actualización y seguridad

Windows Update, recuperación, copia seg.





A partir de aquí solo es necesario seguir el asistente para realizar copias de seguridad de archivos concretos o de todo el sistema.



Tanto la programación de las copias de seguridad o la restauración en su caso, se realiza de la misma manera sencilla y segura y permite mantener a salvo nuestros datos más preciados.



6.- POLÍTICAS ORIENTADAS A LOS USUARIOS INTERNOS(continúa)

- l) Con respecto a los **Correos electrónicos**: El correo electrónico institucional es exclusivo para mensajes de datos relacionados con las actividades de la Institución, no se hará uso de él para fines personales como registro en redes sociales, registros en sitios web comerciales o entablar comunicaciones en asuntos no relacionados con la Asociación.
- m) La información transmitida a través de las cuentas de correo institucional **NO SE CONSIDERA CORRESPONDENCIA PRIVADA**, y por tanto no es confidencial.
- n) Está **PROHIBIDO** utilizar el correo electrónico institucional para divulgar información **CONFIDENCIAL**, reenviar mensajes con palabras soeces o que falten el respeto o atenten contra la dignidad, el honor y la intimidad de las personas, difundir propaganda política, comercial, religiosa, racista, sexista o discriminatoria en general, reenviar contenido o información que atente contra el pudor y las buenas costumbres, así como la propiedad intelectual.
- o) Es responsabilidad del trabajador o funcionario de todo nivel, depurar su cuenta de correo periódicamente o hacer una copia de seguridad completa de sus correos enviados y recibidos. Si tiene problemas o dudas de cómo hacer dicha tarea, tendrá el apoyo del Área de Sistemas.
- p) Con respecto al **uso de Internet**: No se harán descargas de archivos por Internet que no provengan de páginas conocidas o relacionadas con las funciones y actividades de ACENESPAR.
- q) La restricción en el uso de Internet se refiere al acceso a páginas pornográficas conocidas, juegos en línea, redes sociales personales y otras páginas cuyo contenido no es obligatorio para desarrollar las labores encomendadas a cada trabajador o funcionario de todo nivel.



- r) ACENESPAR se reserva el derecho a registrar los accesos restringidos a Internet y a monitorear el contenido al que el usuario puede acceder a través de Internet desde los recursos y servicios de Internet en la Institución, en cualquiera de sus sedes.
- s) Con respecto a la **Seguridad Física**: Es responsabilidad de los funcionarios y trabajadores velar por la conservación física de los equipos de cómputo a ellos asignados, haciendo un adecuado uso de ellos sin maltratar, golpear o romper parte o todo equipo y usarlo exclusivamente para ejercer labores relacionadas con la Institución.
- t) Asimismo, deben reportar inmediatamente a la Gerencia General o Directivos la detección de riesgos reales o potenciales sobre los equipos de cómputo como filtraciones o caídas de agua, producto de las lluvias, riesgo de cortocircuitos o chispas, caídas o golpes sobre los equipos de cómputo, peligro de incendio, robo u otro siniestro, para tomar las medidas correctivas del caso.
- u) Es responsabilidad de todo usuario de equipo informático, que mientras opera sus equipos, no deberá consumir alimentos ni ingerir bebidas.
- v) Debe evitarse colocar objetos encima de los equipos de cómputo, que obstruyan las salidas de ventilación del CPU.
- w) Ningún usuario debe descargar y/o utilizar información, archivos, imagen, sonido, software u otros que estén protegidos por derechos de autor.
- x) Los usuarios que tengan información en medios extraíbles, deben protegerlos del acceso físico y lógico y que el contenido esté libre de virus o software malicioso, usando el antivirus institucional vigente.
- y) Con respecto al **Personal de Sistemas**: El control de los equipos informáticos debe estar bajo la responsabilidad del área de Sistemas, tanto en la asignación de usuarios como la ubicación física.



- z) El área de Sistemas deberá tener el control total y sistematizado de los recursos tecnológicos tanto de hardware como de software para lo cual contará con el apoyo del área de Bienes Patrimoniales.
- aa) El área de Sistemas es la única autorizada para realizar copias de software original, en los casos que amerite. Asimismo, deberá custodiar los manuales, licencias, medios magnéticos u ópticos que acompañen a las versiones ORIGINALES de software.
- bb) Las publicaciones que se realizan en el sitio WEB de la Institución, si bien es cierto lo maneja el área de Imagen bajo el control de las Gerencias y la Presidencia, deben cumplir las especificaciones modernas de toda página web como compatibilidad con todos los navegadores, facilidad de navegación y rapidez al cargar páginas y gráficos.
- cc) El acceso a los sistemas de información y red de datos será a través de nombres de usuario y contraseñas.
- dd) Se debe realizar mantenimiento lógico preventivo a los equipos de cómputo cada 6 meses y mantenimiento físico preventivo mínimo una vez por año.
- ee) Deberá notificarse al área de Sistemas las novedades de vinculación y desvinculación de personal de ACENESPAR con el fin de crear o cancelar accesos a los sistemas de Información, correo electrónico y red de datos.



7.- POLÍTICAS ORIENTADAS A LOS USUARIOS EXTERNOS

- a) El acceso de terceras personas a ACENESPAR debe ser controlado y su ingreso a las diferentes oficinas debe ser autorizado por los funcionarios o personal a cargo de dichas oficinas.
- b) El acceso a las redes Wi-Fi debe ser controlado a través de contraseña para evitar que personas ajenas a la Institución hagan uso de la red de datos de ACENESPAR.

8.- POLÍTICAS DE ADMINISTRACIÓN DE LOS BACKUPS

a) La información Institucional se compone por aquellos datos generados por las operaciones realizadas en cada una de las oficinas y Sedes de la Institución, y su producción, almacenamiento y gestión está a cargo de cada uno de los funcionarios y trabajadores de cada área u oficina.

b) En el capítulo anterior se mencionaron los pasos para realizar los backups de sus equipos de cómputo, ya sea que tengan Windows 7 o Windows 10. Ante cualquier duda consulte siempre con el Área de Sistemas.

c) Las Bases de Datos son el conjunto de datos pertenecientes a los diferentes Sistemas de Información en ACENESPAR y serán respaldados según la periodicidad indicada en el siguiente cuadro:

TIPO DE INFORMACIÓN	FRECUENCIA DE COPIA
Información Institucional	Una vez por semana
Bases de Datos	Interdiario
Archivos de Restauración	Diario

d) Las copias de Seguridad generadas serán almacenadas en un disco duro externo adquirido para tal fin y será resguardado por el responsable del Área de Sistemas.



9.- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL SITIO WEB

- a) El sitio web de ACENESPAR tiene un hosting y un dominio. El dominio es como la partida de nacimiento del sitio web en Internet donde está su “nombre y apellidos completos” que en nuestro caso es “acenespargc.com”. Y el hosting es como decir la “casa donde vive nuestro sitio web”. En nuestro caso, el hosting es administrado por la empresa BLUEHOST, compañía americana, que por el momento nos condiciona el diseño de la web en WordPress, lo cual es un limitante.
- b) Debido a ello, la seguridad de la página está en manos de dicha empresa. Se sugiere MIGRAR a una empresa peruana que cuente con soporte 24/7 es decir las 24 horas del día los 7 días de la semana y con flexibilidad de diseño.
- c) Recientemente se adquirió el certificado SSL que es un título digital que autentifica la identidad de un sitio web y cifra con tecnología SSL la información que se envía al servidor. Es un “pasaporte “electrónico para las transacciones vía web y un elemento importante de Seguridad.
- d) Cuando el usuario hace sugerencias para mejorar los contenidos, información y servicios que ofrece ACENESPAR, dichos aportes llegan al correo webacenespar@gmail.com que es visualizado por el área de Imagen y consultado a las Gerencias por algún detalle en particular.



Información del dominio

Nombre: ACENESPARGC.COM

ID del dominio del Registro: 1931306076_DOMAIN_COM-VRSN

Estado del dominio:

[transferencia de cliente prohibida](#)

Servidores de nombres:

NS1.BLUEHOST.COM

NS2.BLUEHOST.COM

Fechas

Vencimiento del registro: 2026-05-21 22:45:41 UTC

Fecha de actualización: 2025-05-21 15:28:26 UTC

Fecha de creación: 2015-05-21 22:45:41 UTC

Información del registrador

Nombre: Bluehost Inc.

ID de la IANA: 1154

Correo electrónico de contacto para casos de uso indebido: dominio.operaciones@web.com

Teléfono de contacto para casos de uso indebido: tel:+1.8777228662

Información de las DNSSEC

Delegación firmada: No firmado

Servidores autorizados

URL del servidor de registro: <https://rdap.verisign.com/com/v1/domain/acenespargc.com>

Última actualización desde la base de datos del RDAP del registro: 2025-09-09T17:15:58Z

URL del servidor de registrador: <https://rdap.web.com/rdap/domain/ACENESPARGC.COM>

Avisos y comentarios

Avisos:

Condiciones de servicio

Servicio sujeto a Términos de Uso.

<https://www.verisign.com/nombres-de-dominio/protocolo-de-acceso-a-datos-de-registro/terminos-de-servicio/index.xhtml>

Códigos de estado

Para obtener más información sobre los códigos de estado del dominio, visita <https://icann.org/epp>

<https://icann.org/epp>

Formulario de queja por inexactitud del RDD

URL del formulario de queja por inexactitud del RDD de la ICANN: <https://icann.org/wicf>

<https://icann.org/wicf>



acenespargc.com

Actualizado hace 1 segundo ↻



Información del dominio

Dominio:	acenespargc.com
Registrado el:	21 de mayo de 2015
Caduca el:	21 de mayo de 2026
Actualizado el:	21 de mayo de 2025
Estado:	transferencia de clientes prohibida
Servidores de nombres:	ns1.bluehost.com ns2.bluehost.com



Información del registrador

Registrador:	Bluehost Inc.
ID de IANA:	1154
Correo electrónico de abuso:	dominio.operaciones@web.com
Teléfono de abuso:	+1.8777228662



10.-POLÍTICAS DE MANEJO Y ADMINISTRACIÓN DE LAS REDES SOCIALES CORPORATIVAS

a) El manejo y administración de las redes sociales corporativas está a cargo del área de Imagen a través de su Community Manager que se dedica a visualizar las publicaciones, comentarios y réplicas en las diferentes redes sociales, coordinando con las Gerencias y en casos muy puntuales con la Presidencia sobre actividades, logros, metas que deban publicarse o publicitarse mediante estos medios electrónicos.

b) El área de Sistemas interviene en los casos de amenazas en ciberseguridad a través de la identificación, protección, detección, respuesta y recuperación ante estas actividades delictivas y con las herramientas disponibles.

11.- CUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD INFORMÁTICA

a) La Gerencia General, las Gerencias de Sedes, el Director del Colegio Horacio Patiño y los Jefes de Área son responsables de conocer y hacer conocer al personal bajo su mando sobre estas PSI y asegurar su implementación, así como el cumplimiento de estas políticas por parte de su equipo de colaboradores bajo su mando.

b) El Área de Sistemas, estará siempre atento a cualquier duda, dificultad o retraso en el cumplimiento de alguna de las políticas planteadas en el presente Manual.

Surco, 01 de agosto del 2025

Marco Gonzales Borja