5. Controles Basados en Normativas para los riesgos identificados

1. Ataque de Denegación de Servicio (DoS)

ISO/IEC 27001:

- A.13.2.1 Protección contra software malicioso.
- A.13.2.2 Gestión de vulnerabilidades técnicas.
- A.14.1.2 Gestión de la capacidad y el rendimiento de los sistemas de información.

2. Acceso No Autorizado a Servidores Web

ISO/IEC 27001:

- A.9.4.1 Restricción del acceso a la información.
- A.13.1.1 Uso de contraseñas.
- A.13.2.1 Protección contra software malicioso.

NIST CSF:

- PR.AC - Control de acceso.
- DE.CM - Gestión de la configuración.
    a. CIS Controls:Control de Inventario y Activos de Software.
    b. Control de Inventario y Activos de Hardware.

3. Pérdida de Datos por Desastres Naturales

ISO/IEC 27001:

- A.16.1.1 Planificación de la continuidad del negocio.
- A.16.1.4 Pruebas, ejercicios y simulacros del plan de continuidad del negocio.

NIST CSF:

- RS.RP - Plan de recuperación.
- RS.CO - Coordinación de comunicaciones.
    a. CIS Controls:Recuperación de la información.

4. Filtración de Datos a través de Terceros

ISO/IEC 27001:A.15.1.1 Seguridad en los acuerdos con terceros.

- A.15.1.2 Gestión de los servicios de terceros.

NIST CSF:

- SC.SP - Protección de la cadena de suministro.
- PR.DS - Seguridad de los datos.
    a. CIS Controls:Gestión de proveedores.

6. Control y mitigación de riesgos identificados en USPS

Amenaza	Controles y mitigaciones	Roles y Responsabilidades
Ataque de Denegación de Servicio (DoS)	Firewall con reglas de filtrado avanzadas.	Equipo de Seguridad de Red. Administrador de Firewall.
	Sistema de Detección y Prevención de Intrusiones (IDPS).	Equipo de Seguridad de Red. Analista de seguridad
	Análisis de vulnerabilidades y pruebas de penetración.	Equipo de Seguridad de Aplicaciones. Analista de Seguridad.
Acceso No Autorizado a Servidores Web	Políticas de contraseñas robustas.	Equipo de Seguridad. Administrador de Sistemas.
	Autenticación de dos factores.	Administrador de Identidad y Acceso. Equipo de Seguridad.
	Control de acceso basado en roles.	Administrador de Identidad y Acceso. Equipo de Seguridad.
Pérdida de Datos por Desastres Naturales	Plan de recuperación ante desastres detallado.	Equipo de Continuidad de Negocio. Equipo de Operaciones de TI.
	Sitio de respaldo o replicación de datos.	Arquitecto de Infraestructura. Administrador de Sistemas.
Filtración de Datos a través de Terceros	Evaluación de riesgos de seguridad de terceros.	Equipo de Seguridad. Oficial de Cumplimiento.
	Contratos con cláusulas de seguridad detalladas.	Departamento Legal. Equipo de Seguridad.
	Auditorías de seguridad periódicas a terceros.	Auditor Interno. Equipo de Seguridad.

7. Plan de Implementación de Controles de Seguridad para los riesgos de USPS

Políticas de seguridad de la información:

- 5.1.1: **Políticas para la seguridad de la información**

Un conjunto de políticas para la seguridad de la información debería ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas relevantes.

- 5.1.2: **Revisión de las políticas para la seguridad de la información**

Las políticas de seguridad de la información deberían revisarse a intervalos planificados o siempre que se produzcan cambios significativos, a fin de asegurar que se mantenga su idoneidad, adecuación y eficacia.

Organización de la Seguridad de la Información:

- 6.1.1: **Roles y responsabilidades en seguridad de la información**

Todas las responsabilidades en seguridad de la información deberían definirse y asignarse.

- 6.1.2: **Segregación de tareas**

Las funciones y áreas de responsabilidad deberían segregarse para reducir la posibilidad de que se produzcan modificaciones no autorizadas o no intencionadas o usos indebidos de los activos de la organización.

- 6.1.3: **Contacto con las autoridades**

Deberían mantenerse los contactos apropiados con las autoridades pertinentes.

- 6.1.4: **Contacto con grupos de interés especial**

Deberían mantenerse los contactos apropiados con grupos de interés especial, u otros foros y asociaciones profesionales especializados en seguridad.

- 6.1.5: **Seguridad de la información en la gestión de proyectos**

La seguridad de la información debería tratarse dentro de la gestión de proyectos, independientemente de la naturaleza del proyecto.

Seguridad en los Recursos Humanos

- 7.1.1: **Investigación de antecedentes**

La comprobación de los antecedentes de todos los candidatos al puesto de trabajo se debería llevar a cabo de acuerdo con las leyes, normativa y códigos éticos que sean de aplicación y debería ser proporcional a las necesidades del negocio, la clasificación de la información a la que se accede y los riesgos percibidos.

- 7.1.2: **Términos y condiciones del empleo**

Cómo parte de sus obligaciones contractuales, los empleados y contratistas deberían establecer los términos y condiciones en su contrato de trabajo en lo que respecta a la seguridad de la información, tanto hacia el empleado como hacia la organización.

- 7.2.1: **Concienciación, educación y capacitación en seguridad de la información**

Todos los empleados de la organización y, cuando corresponda, los contratistas, deberían recibir una adecuada educación, concienciación y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según corresponda a su puesto de trabajo.

Gestión de Activos

- 8.1.1: **Inventario de activos**

La información y otros activos asociados a la información y a los recursos para el tratamiento de la información deberían estar claramente identificados y debería elaborarse y mantenerse un inventario.

- 8.1.2: **Propiedad de los activos**

Todos los activos que figuran en el inventario deberían tener un propietario.

- 8.1.3: **Uso aceptable de los activos**

Se deberían identificar, documentar e implementar las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

- 8.1.4: **Devolución de activos**

Todos los empleados y terceras partes deberían devolver todos los activos de la organización que estén en su poder al finalizar su empleo, contrato o acuerdo.

Criptografía

- 10.1.1: **Política de uso de los controles criptográficos**

Se debería desarrollar e implementar una política sobre el uso de los controles criptográficos para proteger la información.

- 10.1.2: **Gestión de claves**

Se debería desarrollar e implementar una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

Seguridad Física y del Entorno

- 11.1.1: **Perímetro de seguridad física**

Se deberían utilizar perímetros de seguridad para proteger las áreas que contienen información sensible así como los recursos de tratamiento de la información.

- 11.1.2: **Controles físicos de entrada**

Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados, para asegurar que únicamente se permite el acceso al personal autorizado.

- 11.1.3: **Seguridad de oficinas, despachos y recursos**

Para las oficinas, despachos y recursos, se debería diseñar y aplicar la seguridad física.

Seguridad en las Operaciones

- 12.1.1: **Documentación de procedimientos de los operación**

Deberían documentarse y mantenerse procedimientos de operación y ponerse a disposición de todos los usuarios que los necesiten.

- 12.1.2: **Gestión de cambios**

Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deberían ser controlados.

- 12.1.3: **Gestión de capacidades**

Se debería supervisar y ajustar la utilización de los recursos, así como realizar proyecciones de los requisitos futuros de capacidad, para garantizar el rendimiento requerido del sistema.

Seguridad en las Comunicaciones

- 13.1.1: **Controles de red**

Las redes deberían ser gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

- 13.1.2: **Seguridad de los servicios de red**

Se deberían identificar los mecanismos de seguridad, los niveles de servicio, y los requisitos de gestión de todos los servicios de red y se deberían incluir en cualquier acuerdo de servicios de red, tanto si estos servicios se prestan dentro de la organización como si se subcontratan.

- 13.1.3: **Segregación en redes**

Los grupos de servicios de información, los usuarios y los sistemas de información deberían estar segregados en redes distintas.

Adquisición, Desarrollo y Mantenimiento de Sistemas

- 14.1.1: Análisis de requisitos y especificaciones de seguridad de la información

Los requisitos relacionados con la seguridad de la información deberían incluirse en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

- 14.1.2: Asegurar los servicios de aplicaciones en redes públicas

La información involucrada en aplicaciones que pasan a través de redes públicas debería ser protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificación no autorizadas.

- 14.1.3: Protección de las transacciones de servicios de aplicaciones

La información involucrada en las transacciones de servicios de aplicaciones debería ser protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación, o reproducción de mensaje no autorizadas.

Relaciones con Proveedores

- 15.1.1: **Política de seguridad de la información en las relaciones con los proveedores**

Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deberían acordarse con el proveedor y quedar documentados.

- 15.1.2: **Requisitos de seguridad en contratos con terceros**

Todos los requisitos relacionados con la seguridad de la información deberían establecerse y acordarse con cada proveedor que puede acceder, tratar, almacenar, comunicar, o proporcionar componentes de la infraestructura "Tecnología de la Información".

- 15.1.3: **Cadena de suministro de tecnología de la información y de las comunicaciones**

Los acuerdos con proveedores deberían incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y las comunicaciones y con la cadena de suministro de productos.

Gestión de Incidentes de Seguridad de la Información

- 16.1.1: **Responsabilidades y procedimientos**

Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.

- 16.1.2: **Notificación de los eventos de seguridad de la información**

Los eventos de seguridad de la información se deberían notificar por los canales de gestión adecuados lo antes posible.

Cumplimiento

- 18.1.1: **Identificación de la legislación aplicable y de los requisitos contractuales**

Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la organización para cumplirlos, deberían definirse de forma explícita, documentarse y mantenerse actualizados para cada sistema de información de la organización.

- 18.1.2: **Derechos de propiedad intelectual (DPI)**

Deberían implementarse procedimientos adecuados para garantizar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.