Introduccion

1.1. Contexto

- Descripción del entorno: El Servicio Postal de los Estados Unidos (USPS) es una entidad gubernamental independiente con la responsabilidad de proporcionar servicios postales fiables y asequibles a todos los ciudadanos y empresas de los Estados Unidos.
- Importancia de la ciberseguridad: Dada la naturaleza crítica de su infraestructura y la gran cantidad de datos que maneja, el USPS es un objetivo atractivo para ataques cibernéticos. La protección de la información y la continuidad de las operaciones son fundamentales.
- Necesidad de un SGSI: Un SGSI robusto es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información, así como para cumplir con las regulaciones 1 y normativas aplicables.

1.2. Objeto del documento

- Propósito del documento: Este documento tiene como objetivo establecer las políticas y procedimientos de seguridad que guiarán la implementación y gestión del SGSI en el USPS.
- Declaración de intenciones: Describe el compromiso del USPS con la seguridad de la información ydefine los objetivos generales del SGSI.
- Marco de referencia: Sirve como marco de referencia para todas las actividades relacionadas con la seguridad de la información en la organización.

1.3. Alcance

- Delimitación de los activos: Define claramente los activos de información que están incluidos dentro del alcance del SGSI. Esto puede incluir sistemas, aplicaciones, datos, infraestructura física y personal.
- Procesos y actividades: Identifica los procesos y actividades que se ven afectados por las políticas y procedimientos de seguridad.
- Exclusiones: Especifica cualquier exclusión o limitación en el alcance del SGSI.

1.4. Ámbito de aplicación

- Usuarios: Determina a quiénes se aplican las políticas y procedimientos de seguridad. Esto puede incluir empleados, contratistas, proveedores y otras partes interesadas que tengan acceso a los activos de información del USPS.
- Ubicaciones: Especifica las ubicaciones geográficas o áreas de operación donde se aplican las políticas y procedimientos de seguridad.

1.5. Vigencia y revisiones

- Periodicidad de las revisiones: Establece la frecuencia con la que se revisarán y actualizarán las políticas y procedimientos de seguridad. Esto debe ser al menos una vez al año o cuando ocurran cambios significativos en el entorno o en las regulaciones.
- Proceso de revisión: Describe el proceso para revisar y actualizar el documento, incluyendo quiénes son los responsables y cómo se aprueban los cambios.

1.6. Referencias

- Normativas y leyes: Enumera las normativas, leyes y estándares de seguridad que son relevantes para el USPS, como el NIST Cybersecurity Framework, FISMA, HIPAA (si aplica), etc.
- Otros documentos: Incluye referencias a otros documentos internos o externos que sean relevantes para el SGSI.

2. Principios

- Confidencialidad: Garantizar que la información solo sea accesible para personas autorizadas.
- Integridad: Asegurar que la información sea precisa y completa, y que no pueda ser alterada sin autorización.
- Disponibilidad: Garantizar que la información y los sistemas estén disponibles para los usuarios autorizados cuando los necesiten.
- Responsabilidad: Asignar responsabilidades claras para la seguridad de la información.
- Cumplimiento: Cumplir con todas las leyes, regulaciones y estándares de seguridad aplicables.
- Mejora continua: Establecer un proceso para la revisión y mejora continua del SGSI.

3. Organización de seguridad

- Roles y responsabilidades: Definir los roles y responsabilidades en materia de seguridad de la información, incluyendo el responsable del SGSI, los administradores de sistemas, los usuarios, etc.
- Comité de seguridad: Establecer un comité de seguridad que supervise la implementación y gestión del SGSI.

4. Marco normativo de seguridad

- Políticas de seguridad: Desarrollar políticas de seguridad que abarquen todos los aspectos de la seguridad de la información, como el acceso a sistemas, la gestión de contraseñas, la seguridad de redes, la protección contra malware, etc.
- Procedimientos de seguridad: Establecer procedimientos detallados para implementar las políticas de seguridad.
- Estándares de seguridad: Adoptar estándares de seguridad reconocidos, como ISO 27001 o NIST Cybersecurity Framework.

5. Planes estratégicos

- Análisis de riesgos: Realizar análisis de riesgos periódicos para identificar las amenazas y vulnerabilidades que podrían afectar la seguridad de la información del USPS.
- Plan de tratamiento de riesgos: Desarrollar planes para mitigar o gestionar los riesgos identificados.
- Plan de respuesta a incidentes: Establecer un plan para responder a incidentes de seguridad de manera efectiva.
- Plan de continuidad de negocio: Desarrollar un plan para garantizar la continuidad de las operaciones en caso de un incidente de seguridad o desastre.
- Plan de concientización y capacitación: Implementar programas de concientización y capacitación para educar a los usuarios sobre seguridad de la información.

6. Auditoría

- Auditorías internas: Realizar auditorías internas periódicas para evaluar la eficacia del SGSI y el cumplimiento de las políticas y procedimientos de seguridad.
- Auditorías externas: Contratar auditores externos independientes para realizar auditorías periódicas del SGSI.
- Seguimiento de las recomendaciones: Establecer un proceso para el seguimiento y la implementación de las recomendaciones de las auditorías.

Reglamento de Control de Acceso

Introducción

El reglamento de control de acceso es un documento que establece las normas y procedimientos para gestionar el acceso a los recursos de una organización. Su objetivo principal es garantizar la seguridad de la información y los activos, permitiendo el acceso solo a usuarios autorizados y restringiendo el acceso a información sensible o áreas restringidas.

1.1. Objeto del documento

- Propósito del reglamento: El objeto de este reglamento es definir y establecer el marco normativo para el control de acceso a los recursos de [nombre de la organización], con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, así como la protección de los activos.

1.2. Ámbito de aplicación

- Este reglamento es de aplicación a todos los empleados, contratistas, proveedores y terceros que tengan acceso a los recursos de [nombre de la organización], ya sean estos recursos físicos o lógicos.

1.3. Vigencia y derogaciones

- El presente reglamento entrará en vigor a partir de su fecha de aprobación y deroga cualquier otra disposición anterior que se oponga a su contenido.
- El reglamento será revisado y actualizado periódicamente para asegurar su adecuación a las necesidades de la organización y a los cambios en el entorno.

1.4. Referencias

- Este reglamento se basa en las mejores prácticas de seguridad de la información, normas y estándares internacionales como ISO 27001, NIST Cybersecurity Framework, así como en la legislación vigente en materia de protección de datos.

1.5. Definiciones

- Glosario de términos: Se incluyen definiciones de los términos clave utilizados en el reglamento, tales como acceso, usuario, recurso, autenticación, autorización, etc.

1.5. Definiciones

- Glosario de términos: Se incluyen definiciones de los términos clave utilizados en el reglamento, tales como acceso, usuario, recurso, autenticación, autorización, etc.

2. Controles de seguridad

2.1. Gestión de la identidad

- Se establece un sistema de gestión de identidades para la identificación y autenticación de los usuarios que acceden a los recursos de la organización. Este sistema asigna a cada usuario una identidad única y gestiona sus credenciales de acceso.

2.2. Principios de control de acceso

- Los principios básicos: Se definen los principios fundamentales que rigen el control de acceso, tales como el principio de mínimo privilegio, el principio de necesidad de saber, la segregación de funciones y la responsabilidad.

2.3. Provisión, revocación y modificación de permisos de acceso

- Se establecen los procedimientos para la provisión, revocación y modificación de los permisos de acceso de los usuarios a los recursos de la organización. Esto incluye la solicitud de acceso, la aprobación, la asignación de permisos, la revisión periódica y la revocación de accesos cuando un usuario ya no los necesita.

2.4. Control de acceso físico

- Protección de espacios físicos: Se establecen medidas de control de acceso físico para proteger las instalaciones y áreas restringidas de la organización.

2.4.1. Sistemas de control de acceso físico

- Se utilizan sistemas de control de acceso físico, tales como tarjetas de acceso, lectores biométricos, cerraduras electrónicas y sistemas de vigilancia, para restringir el acceso a personas no autorizadas.

2.4.2. Mecanismos de control de acceso físico

- Barreras físicas: Se emplean mecanismos de control de acceso físico, tales como puertas, vallas, barreras y guardias de seguridad, para proteger las instalaciones y áreas restringidas.

2.5. Control de acceso lógico

- Protección de sistemas y datos: Se implementan medidas de control de acceso lógico para proteger los sistemas de información y los datos de la organización.

2.5.1. Principios de acceso seguro a los sistemas de información

- Solo acceso autorizado: Se aplican principios de acceso seguro a los sistemas de información, tales como la autenticación de usuarios, la autorización de acceso y la gestión de sesiones.

2.5.2. Revisión de permisos de acceso

‘

- Se realizan revisiones periódicas de los permisos de acceso de los usuarios para asegurar que solo tengan acceso a los recursos que necesitan para realizar sus funciones.

2.5.3. Inicio de sesión e inactividad

- Se establecen políticas para el inicio de sesión en los sistemas de información, incluyendo la duración de las sesiones y las medidas de seguridad en caso de inactividad.

2.5.4. Factores de autenticación

- Se utilizan diferentes factores de autenticación, tales como contraseñas, tokens de seguridad, certificados digitales y autenticación biométrica, para verificar la identidad de los usuarios que acceden a los sistemas de información.

2.5.5. Control de acceso de cuentas privilegiadas

- Cuidado con los accesos especiales: Se establecen controles de acceso especiales para las cuentas privilegiadas que tienen acceso a información y funciones críticas de la organización.

2.5.6. Control de acceso a las redes de comunicaciones

- Protección de la red interna: Se implementan medidas de control de acceso a las redes de comunicaciones para proteger la red interna de la organización de accesos no autorizados.

2.5.7. Control de acceso al código fuente

- Protección del código: Se establecen controles de acceso al código fuente de los sistemas de información para proteger la propiedad intelectual de la organización y evitar modificaciones no autorizadas.

Indice de gestión de incidentes

1.1. Objeto del documento

- Propósito del reglamento: Describir el propósito del reglamento de gestión de incidentes como un componente clave del SGSI para el USPS.
- Alcance del reglamento: Indicar que este reglamento se enfoca en la gestión de incidentes de ciberseguridad y otros tipos de incidentes que puedan afectar la seguridad de la información del USPS.

1.2. Ámbito de aplicación

- Especificar que este reglamento aplica a todos los empleados, contratistas y terceros que tengan acceso a los sistemas y datos del USPS.
- Procesos críticos: Identificar los procesos críticos del USPS que están cubiertos por este reglamento, como el procesamiento de correo, la gestión de la cadena de suministro, etc.

1.3. Auditoría Interna

- Detallar cómo las auditorías internas evaluarán la efectividad del reglamento de gestión de incidentes y el cumplimiento de los procedimientos establecidos.
- Frecuencia y alcance: Especificar la frecuencia con la que se realizarán las auditorías y el alcance de las mismas.

1.4. Vigencia y derogaciones

- Indicar la fecha de entrada en vigor del reglamento y qué normativas anteriores quedan derogadas.
- Proceso de revisión: Describir el proceso para la revisión y actualización periódica del reglamento.

1.5. Referencias

- Enumerar las normativas, estándares (ISO 27001, NIST, etc.) y leyes que sirven de base para el reglamento.
- Documentación interna: Incluir referencias a otros documentos internos del USPS que sean relevantes.

1.6. Definiciones

- Glosario de términos: Definir los términos clave utilizados en el reglamento, como incidente, evento, crisis, ciberincidente, etc.
- Terminología específica del USPS: Incluir definiciones de términos específicos utilizados en el USPS.

2. Controles de seguridad

2.1. Gestión de los incidentes de seguridad

- Proceso detallado: Describir en detalle el proceso de gestión de incidentes, incluyendo la detección, registro, clasificación, análisis, contención, erradicación, recuperación y lecciones aprendidas.
- Roles y responsabilidades: Definir los roles y responsabilidades de los diferentes equipos y personas involucradas en la gestión de incidentes.

2.1.2. Incidentes de seguridad de la información

- Incidentes no cibernéticos: Cubrir incidentes que no son necesariamente ataques cibernéticos, como la pérdida de dispositivos, el acceso no autorizado a información sensible, etc.

2.1.3. Incidentes de seguridad de las personas

- Amenazas internas: Incluir incidentes relacionados con amenazas internas, como el robo de información por empleados, el sabotaje, etc.

2.1.4. Incidentes de seguridad física

- Seguridad de instalaciones: Abarcar incidentes de seguridad física que puedan afectar la disponibilidad de los sistemas, como robos, incendios, sabotaje a instalaciones, etc.

2.1.5. Eventos de fraude comercial

- Fraude postal: Definir y establecer procedimientos para la gestión de incidentes relacionados con fraudes, como el robo de correo, el fraude postal, etc.

2.2. Gestión de crisis

- Incidentes mayores: Describir el proceso para gestionar crisis o incidentes de gran envergadura que puedan afectar significativamente al USPS, como desastres naturales, ataques cibernéticos masivos, etc.
- Plan de continuidad: Conectar la gestión de crisis con el plan de continuidad del negocio del USPS.

2.3. Aplicación de cambios de emergencia

- Procedimientos de emergencia: Establecer procedimientos para la aplicación de cambios de emergencia en los sistemas, minimizando los riesgos y asegurando la Confidencialidad, integridad y disponibilidad.

2.4. Recopilación de evidencias

- Evidencias forenses: Detallar los procedimientos para la recopilación y preservación de evidencia digital y física en caso de incidentes de seguridad, siguiendo las mejores prácticas forenses.

2.5. Violaciones de seguridad de datos de carácter personal

- Datos de clientes: Detallar los procedimientos específicos para la gestión de incidentes relacionados con la violación de seguridad de datos personales de clientes o empleados, incluyendo la notificación a las autoridades y a los interesados, de acuerdo con las leyes de protección de datos aplicables.

Índice de Backup y Recuperación de Datos

1.1 Objeto y ámbito de aplicación

- Propósito del plan: Describir el propósito del plan de backup y recuperación como un componente clave del SGSI para el USPS.
- Alcance del plan: Indicar qué tipos de datos están cubiertos por el plan (datos de clientes, información financiera, registros de operaciones, etc.), qué sistemas y ubicaciones se incluyen, y a quiénes aplica el plan (empleados, contratistas, etc.).

1.2 Vigencia y derogaciones

- Indicar la fecha de entrada en vigor del plan y qué normativas anteriores quedan derogadas.
- Proceso de revisión: Describir el proceso para la revisión y actualización periódica del plan, incluyendo la frecuencia y los responsables.

1.3 Referencias

- Enumerar las normativas, estándares (ISO 27001, NIST, etc.) y leyes que sirven de base para el plan.
- Documentación interna: Incluir referencias a otros documentos internos del USPS que sean relevantes, como políticas de seguridad, planes de continuidad, etc.

2. Responsabilidades

- Roles y responsabilidades: Definir claramente los roles y responsabilidades de las diferentes personas o equipos involucrados en el plan de backup y recuperación, incluyendo:
- Responsable del plan: ¿Quién es el encargado de supervisar y mantener el plan?
- Administradores de sistemas: ¿Quiénes son responsables de implementar y gestionar los backups?
- Usuarios: ¿Qué responsabilidades tienen los usuarios en la protección de sus datos?
- Equipo de respuesta a incidentes: ¿Cómo se integra el plan de backup y recuperación con el plan de respuesta a incidentes?

3. Desarrollo

3.1 Planificación

- Análisis de riesgos: Describir cómo se realizó un análisis de riesgos para identificar los datos críticos y los posibles escenarios de pérdida de datos (fallas de hardware, desastres naturales, ataques cibernéticos, etc.).
- Objetivos de recuperación: Definir los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) para cada tipo de dato crítico.
- Estrategias de backup: Detallar las estrategias de backup que se utilizarán (backups completos, incrementales, diferenciales, etc.), la frecuencia de los backups, y los medios de almacenamiento (discos, cintas, nube, etc.).
- Ubicación de los backups: Especificar dónde se almacenarán los backups (sitio primario, sitio secundario, nube), considerando la redundancia y la seguridad física.

3.2 Protección

- Medidas de seguridad: Describir las medidas de seguridad que se implementarán para proteger los backups de accesos no autorizados, modificaciones o eliminaciones malintencionadas (cifrado, control de acceso, protección contra malware, etc.).
- Pruebas de integridad: Establecer procedimientos para verificar periódicamente la integridad de los backups y asegurar que se puedan restaurar correctamente.

3.3 Restauración

- Procedimientos de restauración: Detallar los procedimientos paso a paso para restaurar los datos desde los backups en diferentes escenarios (restauración completa, restauración de archivos individuales, restauración ante desastres, etc.).
- Pruebas de restauración: Establecer la necesidad de realizar pruebas periódicas de restauración para asegurar que los procedimientos sean efectivos y que los datos se puedan recuperar dentro de los RTO y RPO definidos.

3.4 Eliminación y deshecho

- Políticas de retención: Definir políticas de retención de datos que cumplan con los requisitos legales y regulatorios.
- Procedimientos de eliminación segura: Describir los procedimientos para eliminar de forma segura los datos cuando ya no sean necesarios, incluyendo la destrucción de medios de almacenamiento físicos y la eliminación segura de datos en sistemas digitales.

Manual de Concienciación

Introducción

- **Importancia del factor humano:** Enfatizar que la ciberseguridad no es solo tecnología, sino que depende en gran medida del comportamiento de las personas. Un plan de concienciación busca crear una cultura de ciberseguridad en todo el USPS.

- **Riesgos y amenazas:** Mencionar brevemente los principales riesgos y amenazas que enfrenta el USPS, y cómo la falta de concienciación puede aumentar la vulnerabilidad a estos riesgos.

- **Objetivos del plan:** Describir los objetivos generales del plan de concienciación, como aumentar el conocimiento sobre ciberseguridad, promover comportamientos seguros, y reducir el riesgo de incidentes.

2. DISEÑO, EJECUCIÓN Y REVISIÓN DEL PLAN DE FORMACIÓN

2.1. Diseño y Planificación

- Identificación del público objetivo: Definir claramente los diferentes grupos de empleados, contratistas y terceros a los que va dirigido el plan (ej: personal administrativo, personal de TI, gerentes, etc.).

- Análisis de necesidades: Realizar un análisis de las necesidades de cada grupo objetivo en materia de ciberseguridad. ¿Qué conocimientos y habilidades necesitan adquirir o reforzar?

- Definición de temas clave: Seleccionar los temas clave que se abordarán en el plan de concienciación, priorizando los riesgos y amenazas más relevantes para el USPS. Algunos ejemplos:
  - Phishing
  - Malware y ransomware
  - Contraseñas seguras y gestión de acceso
  - Seguridad en dispositivos móviles
  - Ingeniería social
  - Protección de datos personales
  - Políticas de ciberseguridad del USPS
- Selección de métodos y recursos: Elegir los métodos y recursos más adecuados para transmitir los mensajes de ciberseguridad de forma efectiva. Algunas opciones:
  - Formación presencial
  - Cursos online
  - Videos y presentaciones
  - Infografías y materiales impresos
- Establecimiento de indicadores: Definir indicadores concretos y medibles para evaluar la efectividad del plan de concienciación (ej: número de personas capacitadas, resultados de simulacros de phishing, reducción de incidentes de seguridad, etc.).

- Cronograma: Elaborar un cronograma detallado con las actividades de concienciación, fechas, responsables y recursos asignados.

2.2. Ejecución

- Implementación del plan: Poner en marcha las actividades de concienciación según el cronograma establecido, asegurando la participación de los grupos objetivo.
- Comunicación y promoción: Promover activamente el plan de concienciación a través de diferentes canales de comunicación internos para generar interés y participación.
- Seguimiento y registro: Realizar un seguimiento de la participación en las actividades de concienciación y registrar los resultados obtenidos.

2.3. Evaluar y ajustar

- Recopilación de datos: Recopilar datos sobre los indicadores definidos para evaluar la efectividad del plan de concienciación.
- Análisis de resultados: Analizar los resultados obtenidos para identificar áreas de mejora y lecciones aprendidas.
- Ajuste del plan: Ajustar el plan de concienciación en función de los resultados de la evaluación, modificando los temas, métodos, recursos o cronogramas si es necesario.
- Mejora continua: Establecer un proceso de mejora continua para el plan de concienciación, asegurando que se actualice y se adapte a los cambios en el entorno de amenazas y a las necesidades del USPS.