**Incidentes de ciberseguridad**

# Alcance, Contexto, Diseño de política y objetivos

# 

| Enunciado |
| --- |
|
|  |
| Ayuntamiento: Los requisitos funcionales y no funcionales base son:  1) Ya existe cableado de red y electricidad en todas las habitaciones y salas del Ayuntamiento, por lo que se desea evitar inutilizarlas con obras innecesarias.  2) Presupuesto: 20.000€, IVA no incluido para la instalación inicial en el primer año y un 20% adicional, en los 3 años sucesivos, para mantenimiento y mejoras (escalado de la arquitectura).  3) Se deberán proteger 4 habitaciones y una sala de videoconferencias.  4) Empleados: 1 alcalde, 4 concejales, 5 administrativos y 1 técnico informático.  5) Se ha de asegurar que se realiza el tratamiento correcto de la información sensible en el Ayuntamiento atendiendo a legislación vigente (LOPD y RGPD), independientemente del medio de transmisión (correo electrónico, dispositivos de almacenamiento externo, almacenamiento en discos duros de los equipos y servidores, etc). Ya que se tratan los datos de los residentes de la población.  6) No se sabe quién, pero hay antecedentes de que un/a funcionario/a se suele meter en páginas de mala reputación, y abrir correos electrónicos sospechosos por mera curiosidad, lo que ha provocado antecedentes de infección por troyanos y phishing que ha afectado con anterioridad a la reputación del Ayuntamiento. Se desea eliminar este problema de raíz. 7) En el último mes, se ha sufrido un ataque DDoS que inhabilitó el servidor Web del Ayuntamiento justo antes de las elecciones. Se desea evitar esta situación antes de las próximas elecciones (en los próximos 4 años).  8) Se requiere controlar los accesos al edificio, al despacho del alcalde y a la habitación donde está instalado el rack de servidores y dispositivos de red.  9) Sistema operativo preinstalado en los equipos: Windows 10 Pro.  10) El ayuntamiento trabaja con diferentes empresas proveedoras de servicios como son papelería, empresas de equipos informáticos y proveedoras de internet para realizar sus operaciones. |
| Introducción |
| La Política de Seguridad de la Información persigue la adopción de un conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, que constituyen los tres componentes básicos de la seguridad de la información, y tiene como objetivo establecer los requisitos para proteger la información, los equipos y servicios tecnológicos que sirven de soporte para la mayoría de los procesos del Ayuntamiento de Las Palmas de Gran Canaria. |
| Alcance |
| Esta política aplica a todos los integrantes, colaboradores y a todas las personas, independientemente de su cargo o nivel, que trabajan para la Empresa, incluyendo sin limitar, alcalde, concejales, trabajadores varios y, en  general, cualquier colaborador eventual o permanente, así como los particulares. Es aplicable a cualquier trato, contrato o negociación en todos los países donde el organismo tiene operaciones.  Se abordará la **infraestructura**, **procedimientos, servicios y sistemas** de las áreas físicas del edificio central del ayuntamiento de Las Palmas de Gran Canaria, ubicado en la calle León y Castillo, 270 en la localidad de Las Palmas de Gran Canaria. Este abordará específicamente cuatro habitaciones y una sala de videoconferencias en las instalaciones físicas.  Se tomará en cuenta que el edificio ya cuenta con cableado de red y suministro eléctrico funcional, procurando no interrumpir las áreas con obras en la medida de lo posible.  Asimismo, se incorporará el proceso electoral en este Sistema de Gestión de Seguridad de la Información (SGSI). Exclusiones del alcance Destacar que los firmantes no asumen responsabilidad alguna por áreas o ámbitos que se encuentren fuera del área física del edificio central. |
| Contexto |
| Partes relacionadas (responsables) |
| * **Alcalde y Concejales (4):**   + El alcalde y los concejales son los líderes del ayuntamiento y tienen un interés directo en garantizar la seguridad de la información y la infraestructura, ya que esto afecta la efectividad de la administración y la confianza de los ciudadanos. * **Empleados Municipales:**   + Todos los empleados del ayuntamiento, incluyendo administrativos y personal técnico, son partes interesadas, ya que son usuarios y custodios de la información sensible. * **Técnico Informático (1):**   + El técnico informático tiene un papel crucial en la implementación y mantenimiento de medidas de seguridad informática. Su experiencia y acciones afectarán directamente la seguridad de los sistemas. * **Organismos Reguladores:**   + Entidades gubernamentales encargadas de la regulación y cumplimiento de normativas, como la Agencia Española de Protección de Datos (AEPD), son partes interesadas, ya que el ayuntamiento debe cumplir con leyes y regulaciones. * **Ciudadanos en General:**   + Además de los residentes específicos, la población en general tiene un interés en la seguridad del ayuntamiento, ya que la seguridad afecta la calidad de los servicios y la confianza en la administración local. |
| *“La política de seguridad define qué es lo que desea proteger, y los objetivos de seguridad expresan lo que espera de los usuarios del sistema.”*  [*Documentación de IBM*](https://www.ibm.com/docs/es/i/7.5?topic=ssw_ibm_i_75/rzaj4/rzaj40j0securitypolco.html) |
| Políticas |
| Con la finalidad de garantizar la confidencialidad, integridad y disponibilidad de la información, así como la protección de los recursos tecnológicos y humanos del Ayuntamiento, cumpliendo con la normativa vigente y asegurando la continuidad operativa. |
| *Nuestro Sistema de Gestión se apoya en las siguientes directrices para garantizar la eficiencia y calidad de los servicios proporcionados por el Ayuntamiento:*   1. **Garantizar la Disponibilidad y Seguridad de los Servicios:** Nos comprometemos a asegurar la disponibilidad de nuestros servicios municipales, así como a mantener la integridad y seguridad de la documentación correspondiente, cumpliendo con los acuerdos establecidos con los ciudadanos. 2. **Métodos Sistemáticos y Trazabilidad:** Adoptaremos métodos sistemáticos para que las actividades realizadas en el Ayuntamiento sean trazables y reproducibles, garantizando una gestión eficiente y transparente. 3. **Gestión del Conocimiento y Polivalencia del Personal:** Gestionaremos el conocimiento existente sobre nuestros servicios y soluciones, utilizando herramientas adecuadas y promoviendo su compartición entre el personal municipal. Buscamos lograr un equipo con mayor polivalencia en las tareas a realizar para mejorar la eficacia de los servicios públicos. 4. **Cumplimiento de Requisitos Legales y Compromisos:** Nos comprometemos a cumplir con los requisitos establecidos por la legislación aplicable y los compromisos pactados con la comunidad, asegurando la transparencia y la responsabilidad en nuestras acciones. 5. **Establecimiento y Revisión de Objetivos de Calidad:** Estableceremos y revisaremos regularmente objetivos relacionados con la calidad de los servicios, la seguridad de la información y el impacto ambiental. Estos objetivos servirán como base para la mejora continua de nuestras actividades municipales. 6. **Protección del Medio Ambiente y Ahorro Energético:** Nos comprometemos a minimizar los impactos ambientales negativos resultantes de nuestros servicios municipales, manteniendo estándares adecuados para la calidad y la preservación del medio ambiente. Buscamos la protección del entorno y el ahorro energético en todas nuestras operaciones. 7. **Mejora Continua y Orientación al Negocio:** Nos esforzamos por mejorar constantemente nuestros servicios, procesos y el propio Sistema de Gestión, manteniendo una orientación permanente hacia el beneficio de la comunidad y el desarrollo sostenible.   *Para garantizar el cumplimiento de esta Política, la Dirección General del Ayuntamiento se compromete a divulgar entre todo el personal municipal. Cada miembro del equipo debe ser consciente de su responsabilidad en la calidad de su trabajo y su contribución a los objetivos de gestión del Ayuntamiento.* |

| Objetivos |
| --- |
| El objetivo general es diseñar un modelo de un sistema de gestión de la seguridad de la información , que aplique a todos los procesos y áreas de la organización, alineado con la norma NTC2 -ISO3 -IEC4 27001:2013.  Desde la protección de datos hasta la prevención de amenazas, estos objetivos no solo buscan mitigar riesgos, sino también alinearse estratégicamente con los valores organizativos y requisitos normativos. |
| * **Autenticación y autorización**   + Controlar el acceso al edificio con cámaras de vigilancia, sistemas de control de acceso, etc.   + Control y seguridad del acceso al despacho del alcalde y a la habitación con el rack de servidores. * **Velar por la protección de recursos (datos)**   + Cumplir con la legislación vigente (LOPD y RGPD).   + Diagnosticar el estado actual de cumplimiento con respecto a los dominios y objetivos de control de la norma NTC-ISO-IEC 27001:2013.   + Definir un conjunto de políticas y procedimientos para la seguridad de la información aplicadas a todos los procesos actuales de la organización de acuerdo a la norma NTC-ISO-IEC 27001:2013.   + Definir los elementos del modelo del sistema de gestión de la seguridad de la información en todos los procesos de la organización alineado con la norma NTC-ISO-IEC 27001:2013.   + Especificar si se realizará alguna auditoría de seguridad para evaluar el cumplimiento normativo. * **Corregir antecedentes de seguridad informática:**   + Implementar una política de seguridad para tratar los problemas relacionados con el comportamiento de ataques cibernéticos a funcionarios.   + Especificar medidas para prevenir o mitigar ataques DDoS en procesos electorales.   + Establecer un historial de incidentes, estado y resoluciones. * **Establecer un control del presupuesto y mantenimiento:**   + Contemplar el presupuesto destinado al mantenimiento y mejoras y determinar si puede no ser suficiente. * **Establecer políticas de Proveedores y terceros:**   + Definición de políticas de diligentemente debida con de proveedores empresas proveedoras de servicios. * **Planificar la formación del personal técnico** * **Planificar el método y la periodicidad de este documento** |

# Bibliografía

* <https://normaiso27001.es/1-auditoria-inicial-iso-27001-gap-analysis>
* [Documentación IBM respecto a politicas políticas de seguridad](https://www.ibm.com/docs/es/i/7.5?topic=ssw_ibm_i_75/rzaj4/rzaj40j0securitypolco.html)