ANÁLISIS DEL ESTADO ACTUAL SEGURIDAD INFORMÁTICA

Ayto. El Real de la Jara

27/02/2025
EZEQUIEL JIMÉNEZ LÓPEZ

1. RESUMEN

El presente estudio tiene como propósito conocer el estado actual en el que se encuentra el Ayuntamiento de la localidad sevillana de El Real de la Jara respecto a la seguridad informática mediante la elaboración de un análisis basado en el Real Decreto 311/2022, de 3 de mayo por el que se regula el Esquema Nacional de Seguridad (ENS), para identificar los riesgos y las vulnerabilidades a las cuales se encuentra expuesta la información.

Durante el análisis se identificaron los activos y la información básica de los mismos, con el fin de determinar las amenazas y el impacto al que se encuentran expuestos, se realizó revisión de documentación, entrevistas y visitas, para conocer el impacto que puede llegar a tener la materialización de una amenaza.

Como finalidad se presentan posibles soluciones a corto y mediano plazo donde la organización decidirá la implementación de controles de seguridad, en busca de conservar los tres pilares de la seguridad de la información.

2. INTRODUCCIÓN

Para toda organización, empresa, etc… la información es el activo más importante con el que cuenta, es por lo que actualmente se debe concienciar desde la alta dirección que se debe proteger de cualquier evento que la pueda afectar.

Actualmente las organizaciones en el mundo enfrentan un cambio en la forma en que sus empleados acceden a la información, debido a la pandemia generada por el COVID 19 la cual obligo a la virtualización de muchos procesos para los cuales no estaban preparados, pero la necesidad de poder seguir operando llevo a la rápida habilitación de acceso remoto a los diferentes aplicativos e información, sin analizar previamente los riesgos a los que se puede encontrar expuesta en el ciberespacio.

Es por lo que este proyecto tiene como finalidad el análisis del estado actual respecto a la seguridad de la información dentro de la entidad local compuesta por el Ayuntamiento de El Real de la Jara, proponiendo soluciones mediante un plan que ayuden a salvaguardar la integridad, confidencialidad y disponibilidad de la información.

Otro punto importante, o mejor dicho, importantísimo a tener en consideración es la falta de concienciación en ciberseguridad por parte de los empleados, lo que podría llevar a producir consecuencias graves, afectando no solo a la seguridad de la información, sino también a la continuidad de los servicios públicos y la confianza ciudadana. Estas posibles consecuencias incluyen:

Brechas de seguridad: La falta de ciberseguridad puede dar lugar a prácticas inseguras por parte de esos empleados, como contraseñas débiles o el uso descuidado de dispositivos, lo que aumenta el riesgo de brechas de datos.

Interrupción de servicios públicos: Los ataques cibernéticos pueden interrumpir la operación normal de servicios esenciales proporcionados por el ayuntamiento.

Pérdida de confianza ciudadana y daño reputacional: La divulgación de información sensible o la interrupción de servicios puede afectar a la confianza de los ciudadanos en la capacidad del ayuntamiento para proteger sus datos y proporcionar servicios de manera segura así como un grave daño reputacional, afectando su imagen pública.

Costes económicos: La recuperación de un ataque cibernético y la implementación de medidas correctivas pueden generar costes significativos, incluyendo la inversión en recuperación de datos y la reparación de sistemas comprometidos.

Pérdida de datos sensibles: La falta de ciberseguridad también puede llevar a prácticas que exponen datos sensibles, como información financiera o personal de los ciudadanos, a accesos no autorizados.

Para mitigar estas consecuencias, es esencial invertir en programas de concienciación en ciberseguridad, asegurando que todos los empleados del ayuntamiento estén informados, capacitados y comprometidos en prácticas seguras de seguridad informática.

3. ANÁLISIS Y RESULTADO

Para el análisis inicial realizado en el Ayuntamiento de El Real de la Jara, valoramos los controles o medidas de seguridad utilizados y su grado de madurez, es decir, si están implantados y en qué estado están.

Es importante debido a que, al señalar las deficiencias en los controles internos, las políticas, los procedimientos y/o el incumplimiento de estándares y regulaciones, se pueden desarrollar recomendaciones y planes de acción para mitigar los riesgos identificados.

Adicionalmente se busca que el consistorio cumpla con regulaciones y normativas específicas en cuanto a la seguridad de la información y la protección de datos, mediante este análisis, se busca evaluar el grado de cumplimiento de los objetivos de control y controles, se identifican las áreas que necesitan mejoras para alcanzar dicho cumplimiento.

Con lo anterior y utilizando la escala propuesta en la siguiente tabla se analizará el estado de la organización municipal.

Estado	Significado
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte.
Repetible	La medida de seguridad se realiza de un modo totalmente informal (*con procedimientos propios, informales*). La responsabilidad es individual. No hay formación.
Definido	El control se aplica conforme a un procedimiento documentado, pero no aprobado ni por el Responsable de Seguridad ni por el Comité de Dirección.
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente.

A continuación, se presenta el estado de madurez en el que se encuentra el Ayuntamiento tras un análisis inicial.

- **Contexto de la organización:** Se trata del punto de partida para desarrollar el SGSI (*Sistema de Gestión de Seguridad de la Información*) y consiste en determinar o identificar los "*problemas*" internos y externos a los que se enfrenta la organización. Explicado de otra forma, el contexto organizacional consiste en considerar las expectativas y necesidades de todas las partes interesadas.
- **Liderazgo:** El liderazgo en ciberseguridad es más que supervisar las medidas técnicas; es sobre guiar a las personas, crear una cultura de seguridad y tomar decisiones estratégicas que protejan a la organización de amenazas en constante evolución.
- **Planificación:** El plan de ciberseguridad es una estrategia elaborada para saber cómo enfrentarse ante cualquier situación que pueda poner en riesgo la integridad, disponibilidad y confidencialidad de la información.
- **Soporte:** Consiste en tener a su disposición a un especialista para realizar actividades, tanto preventivas cómo reactivas (*orientada a realizar cambios*), con las que se fortalezca la seguridad tecnológica. Así como la adaptación a las necesidades de ciberseguridad específicas en cada caso.
- **Operación:** requisitos para controlar que estamos tomando las medidas adecuadas para lograr los objetivos de la Seguridad de la Información.
- **Evaluación del Desempeño:** Evaluar el rendimiento o efectividad de nuestro SGSI o de la Seguridad de la información.
- **Mejora:** Acciones preventivas y correctivas

Estado actual del Ayuntamiento

Numeral	Requisito	Estado
1	Contexto de la organización	Inicial
2	Liderazgo	Inexistente
3	Planificación	Inexistente
4	Soporte	Administrado
5	Operación	Inicial
6	Evaluación del Desempeño	Inexistente
7	Mejora	Inexistente

Se puede observar que el consistorio solo dispone de un numeral 4, en estado Administrado a través de empresa externa INPRO y cuenta con los numerales 1 y 5 en un estado inicial, lo que indica que la organización empieza a tomar interés por alinearse a lo requerido por la norma, sin embargo, es los numerales 2,3,6 y 7 se encuentran en estado inexistente, es por esto que se hace importante aportar en la implementación de medidas efectivas con el fin de generar un cierre de brechas fortaleciendo la seguridad de la información.

3.1 OCURRENCIAS ENCONTRADAS

3.1 Resumen de criticidad de ocurrencias encontradas

3.1.1 Asignación mínima de responsabilidad sobre los activos.

- Responsable de Seguridad (RSI): 0 - No asignado.
  Encargado de supervisar y aplicar políticas de seguridad, además de coordinar las medidas técnicas necesarias para la protección de la empresa.
- Responsable de Información: 0 - No asignado.
  Encargado de garantizar la protección de los activos de información, incluyendo datos confidenciales, sistemas y redes, contra amenazas y ataques físicos o cibernéticos.

3.1.2 Copias de seguridad.

Se constata un sistema de realización de copias de seguridad siguiendo un plan bien coordinado y estructurado.

Este proceso es realizado a través de la Diputación de Sevilla y la empresa externa INPRO, realizando un backup de manera diaria y de manera redundante, una copia en local en un servidor habilitado a tal efecto instalado en las dependencias del Ayuntamiento al que llaman "*Medusa*" y una segunda copia en un CPD (*Centro de procesamiento de datos*) de la citada empresa, copia que a su vez es replicada en un tercer CPD.

La empresa INPRO nos comunica que en caso de necesidad, el tiempo de resolución desde que una incidencia es comunicada, el proceso de restauración se encontraría en torno a 60 minutos.

3.1.3 Página web.

Al igual que sucede con las copias de seguridad, la empresa INPRO gestiona el diseño y mantenimiento de la página web, el portal de transparencia y la sede electrónica, que permiten el posicionamiento en internet del Ayuntamiento y la relación electrónica con la ciudadanía, siendo también la encargada de la seguridad y protección de estos servicios en la nube.

3.1.4 Sistema Operativo obsoleto.

El 100% de los equipos dispone de un S.O. Microsoft Windows en varias versiones y por ello hay que tener en cuenta que desde el pasado 10 de enero de 2023, Microsoft dejó de ofrecer actualizaciones de seguridad y soporte técnico para Windows 8.1 y por tanto, cualquier otra versión inferior se determina como importante amenaza frente a posibles ciberataques.

El número de activos afectados por al menos una ocurrencia de seguridad de esta categoría es: 6

Dispone de un sistema operativo obsoleto

Descripción detallada

El uso de sistemas tecnológicos que no están actualizados, también conocidos como obsoletos, representa un conjunto de vulnerabilidades que incide en los datos y el bienestar de la entidad, produciendo daños cibernéticos.

- Problemas de incompatibilidad: Una vez que un software deja de recibir actualizaciones, parches y soporte, se da lugar a nuevos malware y virus maliciosos, ya que va perdiendo su capacidad para resistir los ciberataques modernos. También inhabilita la adaptación de nuevas infraestructuras o migraciones de TI, complicando la funcionalidad de un software antiguo con una tecnología más nueva.

Recomendación

Se recomienda actualización a la última versión.

Activos afectados

192.168.x.x Para constatar se encuentra fuera del servidor proxy existente en las instalaciones.

IP	DESPACHO	Versión
192.168.31.154	Municipales	8.1 Pro
192.168.0.13	Juventud	7 Pro
192.168.31.x	Mancomunidad	7 Ultimate
10.180.1.175	Igualdad	7 Pro
10.180.1.60 / 192.168.0.164	Servicios Sociales	7 Pro
192.168.0.36 / 10.180.10.100	Archivo	8.1 Pro

3.1.5 Software antivirus original.

El Ayuntamiento dispone de licencia de un software antivirus EDR de la compañía Kaspersky Lab, en concreto hablamos de Kaspersky Endpoint Security versión 10, aunque existen equipos sin instalación y por tanto sin esta protección.

El número de activos afectados por al menos una ocurrencia de seguridad de esta categoría es: 8 ausencia total – 3 antivirus no licenciados para Ayuntamiento.

No se ha detectado un antivirus.

Recomendación

Realizar instalación de manera urgente en estos equipos.

Activos afectados

192.168.x.x Para constatar se encuentra fuera del servidor proxy existente en las instalaciones.

IP	DESPACHO
192.168.31.154	Municipales
10.180.1.14	Alcaldía
10.180.1.50	Recursos Humanos
10.180.1.57	Urbanismo
192.168.31.x	Coworking - Totem
192.168.31.x	Mancomunidad
192.168.31.x	*Igualdad en coworking - dispone de McAfee*
192.168.0.68	Cultura y Festejos
10.180.1.51	Cultura y Festejos
192.168.0.37	*Bibliotecaria - dispone de McAfee*
192.168.0.36	*Archivo - ESET Antivirus SIN licencia*

3.1.6 Software ofimática original.

** En proceso de análisis. En un principio nos informan existe un paquete de licencias de Microsoft Office. Pendiente de corroborar.*

La mayoría de los activos analizados dispone de instalación de un paquete Microsoft Office Profesional Plus NO ACTIVADO.

El número de activos afectados por al menos una ocurrencia de seguridad de esta categoría es: 14

Paquete Ofimático instalado NO original/activado.

Recomendación

En el caso de disponer de las correspondientes licencias, Activar y Actualizar, en caso contrario, si no se dispone de estas licencias, Desinstalar.

Activos afectados

192.168.x.x Para constatar se encuentra fuera del servidor proxy existente en las instalaciones.

IP	DESPACHO	Versión
192.168.31.154	Municipales	Office Profesional Plus 2013
192.168.0.50	Turismo	Office Profesional Plus 2016
192.168.0.13	Juventud	Office Profesional Plus 2010
10.180.1.162	Administración/Secretaria	Office Profesional Plus 2013
10.180.1.63	Administración/Urbanismo	Office Profesional Plus 2010
10.180.1.14	Alcaldía	Office Profesional Plus 2010
10.180.1.53	(Mª del Carmen)	Office Profesional Plus 2010
10.180.1.50	RRHH	Office Profesional Plus 2010
10.180.1.57	Urbanismo	Office Profesional Plus 2010
10.180.1.23	Secretaría	Office Profesional Plus 2010
10.180.1.151	Trabajador Social	Office Profesional Plus 2010
192.168.0.68	Cultura y Festejos	Office Profesional Plus 2010
10.180.1.51	Cultura y Festejos	Office Profesional Plus 2010
192.168.0.36	Archivo	Office Profesional Plus 2010

3.1.7 Red.

El número de activos afectados por al menos una ocurrencia de seguridad de esta categoría es: 3

No se ha detectado un cortafuegos (Firewall) en ejecución

Descripción detallada
Se ha detectado un activo que parece no estar detrás de un firewall o tiene una mala configuración.
La gestión Firewall se encuentra controlada por el antivirus Kaspersky EDR, por lo que dicha gestión se lleva a cabo a través de un servidor remoto controlado y gestionado por Diputación por la empresa Inpro.

Recomendación
Se recomienda que todos los activos expuestos a Internet estén protegidos por un firewall con la configuración más restrictiva posible y en este caso concreto de las instalaciones del Ayuntamiento de El Real de la Jara, se recomienda la gestión sea procesada por el propio antivirus Kaspersky en su versión EDR, realizando una instalación del mismo, ya que los equipos afectados coinciden en la situación de NO disponer de software antivirus, lo que agrava aún más la situación de falta de un Firewall activo.

Activos afectados

192.168.x.x Para constatar se encuentra fuera del servidor proxy existente en las instalaciones.

IP	DESPACHO
10.180.1.57	Urbanismo
192.168.0.68	Cultura y Festejos
10.180.1.51	Cultura y Festejos

3.1.7.1 Análisis de Red.

Durante el análisis de red, observamos que existe un área del Ayuntamiento, denominada por el mismo como Coworking, en el que ofrecen acceso gratuito a un espacio de trabajo compartido que cuenta con diferentes servicios y amenidades, entre las cuales se incluye acceso a internet.

Para ello existe una red WiFi gratuita conectada a una red de fibra óptica. Esta red, aunque opera en un segmento de red distinto al utilizado por el proxy del Ayuntamiento, se encuentra conectada físicamente a la red local a través de un switch, por lo que cualquier ciudadano que utilice dichas instalaciones gratuitas, disponiendo de los suficientes conocimientos informáticos podría poner en riesgo la seguridad informática y acceder a datos de los equipos del Ayuntamiento.

Recomendación
Dado que la mencionada red wifi se encuentra conectada a una red de fibra independiente de la utilizada por el Ayuntamiento, se recomienda la desconexión física de la red local, de manera que los usuarios que puedan hacer uso de las instalaciones de coworking, sigan disponiendo de conexión a internet pero no puedan comprometer la estabilidad de la intranet local del consistorio.

3.1.7.2 Infraestructura de Red - 5

El Ayuntamiento dispone de una red LAN de reciente instalación mediante cable CAT6 libre de halógenos.

En la parte hardware de red, aunque parte es de reciente implantación con equipos tecnología giga y fttp, aún disponen de switch con tecnología fast Ethernet, pendientes de sustitución mediante un proyecto aprobado en firme en vías de ejecución.

3.2 Control de acceso

El control de acceso a las instalaciones es un componente crucial para obtener certificaciones en normas de ciberseguridad reconocidas.

Importancia del Control de Acceso en Normas de Ciberseguridad:

- **Protección de activos.**
  - Las normas de ciberseguridad, como ISO 27001, enfatizan la protección de los activos de la información. El control de acceso físico es esencial para prevenir el acceso no autorizado a servidores, centros de datos y otras áreas críticas.

- **Gestión de riesgos.**
  - Un control de acceso efectivo reduce el riesgo de incidentes de seguridad causados por intrusiones físicas, robo de equipos o sabotaje.

- **Demostración de Diligencia Debida.**
  - Tener sistemas de control de acceso robustos demuestra que la empresa toma en serio la seguridad de sus instalaciones y datos.

Tras un examen en las instalaciones, se constata que aunque dispone de un control de acceso con reconocimiento facial, NO es utilizado y se mantiene acceso libre a las dependencias.

Recomendación

Se recomienda encarecidamente llevar a cabo un control de acceso a las instalaciones, de manera que cualquier persona que acceda a las dependencias quede registrado un control de acceso con toma de datos compuesto por Nombre completo, documento nacional de identidad y fecha y hora. También sería recomendable adjuntar motivo de visita resumido y despacho.

En cuanto a los empleados del Ayuntamiento y personal de acceso habitual, realizar un control de acceso facial.

3.2 TEST HÁBITOS DE TRABAJO

3.2 Hábitos de trabajo del personal del Ayuntamiento

Kevin Mitnick, uno de los hackers más famosos en la historia de la ciberseguridad comentaba que «*las organizaciones gastan millones en firewalls y dispositivos de seguridad, pero tiran el dinero porque ninguna de estas medidas cubre el eslabón más débil de la cadena de seguridad: las personas que usan y administran los ordenadores*».

Según datos de la Oficina de Seguridad del internauta, OSI en siglas, "*Un 95% de los ciberataques son a causa de errores de usuario.*"

Atendiendo a este elevado porcentaje y centrándonos en esta posible vía de entrada para prevenir posibles ataques, se realiza a cada trabajador de la entidad una serie de preguntas para evaluar los hábitos de trabajo y de esta manera localizar posibles brechas de seguridad. Para ello, nos reunimos independientemente uno por uno, resultando una información valiosa que detallamos a continuación.

- Número de empleados encuestados: 14

- **Tipo de correo electrónico utilizado, personal o corporativo**
    - Personal: Un 14,29% (*2 empleados*) utiliza únicamente correo personal, pero además, manifiestan no disponer de correo corporativo.
    - Personal y además dispone de un corporativo pero no lo utiliza: Un 14.29% (*2 empleados*).
    - Corporativo: Un 14.29% (*2 empleados*) utiliza únicamente correo corporativo.
    - Ambos: Un 57,14€ (*8 empleados*) utiliza ambos tipos de correo.

    ** Como dato ajeno a este estudio pero importante debido a que causa el uso de correos personales, un amplio margen de empleados encuestado hace saber que utilizan correo personal porque el corporativo dispone de poca capacidad.*

Recomendación

Utilización en la medida de lo posible únicamente correos corporativos, pues está ampliamente demostrado que los mails corporativos *ofrecen mayores medidas de seguridad*, control, supervisión, gestión y procesamiento de los datos.

En el caso del Ayuntamiento, Diputación pone a su disposición una herramienta específica que lleva asociado un control de seguridad exhaustivo. Se trata del software GroupWise® de Novell, un sistema de correo electrónico corporativo y compatible con varias plataformas que proporciona seguridad en mensajes, calendarios, programación y mensajes instantáneos.

- **Fortaleza de las contraseñas utilizadas para esos correos**
    - Débil: El 14,29% (*2 empleados*) utiliza sólo letras y sólo números en correo personal.
    - Intermedia:
    - Sólida: El 100% utiliza contraseña segura en correo corporativo.

Recomendación

Las contraseñas son la primera línea de defensa contra el acceso no autorizado de archivos, dispositivos y cuentas en línea. Las contraseñas seguras ayudan a proteger los datos de usuarios y ante software malintencionados. Cuanto más segura sea la contraseña, más protegida estará la información.

Para atender a una política correcta en ciberseguridad, es recomendable establecer un cambio de contraseña cada tres meses.

- **¿Recibe publicidad en los correos?**
    - Si: El 71,43% (*10 empleados*) manifiesta recibir publicidad PERO únicamente en el correo personal.
    - No: El 28,57% (*4 empleados*) manifiesta no recibir publicidad en correo electrónicos.

Recomendación

NUNCA abrir publicidad proveniente de direcciones de correo no conocidas. Marcar como spam y borrar.

- **En caso afirmativo,… ¿la abre?**
    - Si: De los 10 empleados que manifiestan recibir publicidad en el correo, el 20% (*2 empleados*) afirma abrirlos en bastantes ocasiones.
    - No: El resto, el 80% (*8 empleados*), afirma no abrir nunca ningún tipo de publicidad y que proceden a borrar esos correos.

- **¿Alguna vez ha recibido alerta de algún tipo, antivirus, firewall, etc…?**
    - Si:
    - No: el 100% no recibe alerta de virus proveniente del antivirus.

- **Utiliza unidades externas, HD... pendrive?**
    - Si: El 78,57% (*11 empleados*) utiliza pendrive o HD externo. De estos 11 empleados, 5 hacen uso de pendrive de usuarios porque necesitan instalar los certificados digitales, llegando incluso a manifestar uno de los encuestados, que omite el análisis que ofrece el antivirus una vez es insertado en el equipo.
    - No: El resto, 3 empleados no hace uso de estos dispositivos.

Recomendación

NUNCA utilizar un pendrive que provenga de personas ajenas a la corporación. En caso de necesidad de disponer de algún dato que tenga que facilitar un usuario, requisito indispensable que esos datos lo hagan llegar vía correo electrónico.

De igual modo, utilizar pendrive únicamente en los equipos del Ayuntamiento y si necesitásemos utilizar algún tipo de información en equipos externos, sobre todo en otros entornos laborales fuera de las instalaciones del consistorio, hacerlo igualmente vía email.

En el caso de equipos personales y que sea estrictamente necesario, esos equipos deben disponer de licencia antivirus debidamente actualizada. Para ello y dependiendo del área de trabajo, es posible disponer de una licencia Kaspersky utilizable en un equipo personal del responsable del área. Para ello se debe establecer comunicación con la empresa externa INPRO mediante las herramientas habilitadas a tal efecto.

- **En caso afirmativo, dónde más utiliza esa unidad externa.**
    - En ningún otro sitio: El 18,18% (*2 empleados*).
    - En otro trabajo: El 9,09% (*1 empleado*).
    - En equipo personal: El 9,09% (*1 empleado*).
    - En otro trabajo y en equipo personal: El 18,18% (*2 empleados*).
    - Proviene de personas ajenas al Ayuntamiento: El 45,45% (*5 empleados*).