Estrategia de Seguridad de la Dirección General de Informática y Comunicaciones

Manuel Escudero Sánchez
Director General de Informática y Comunicaciones.
Consejería de Economía y Hacienda. Comunidad Autónoma de la Región de Murcia.

Elena González Arnal
Jefe de Servicio de Sistemas Informáticos. Responsable de Seguridad en funciones.
Dirección General de Informática y Comunicaciones. Consejería de Economía y Hacienda. Comunidad Autónoma de la Región de Murcia.

Manuel Frutos Mirete
Subdirector General de Sistemas, Comunicaciones y Redes.
Dirección General de Informática y Comunicaciones. Consejería de Economía y Hacienda. Comunidad Autónoma de la Región de Murcia.

Resumen:

La Dirección General de Informática y Comunicaciones ha considerado desde siempre la seguridad como un proceso fundamental para la consecución de sus objetivos. En los últimos tiempos se ha potenciado en gran medida esta área de trabajo revisando líneas estratégicas, creando una unidad organizativa con competencias exclusivas en esta materia y potenciando el Plan Estratégico de Seguridad alineándolo con el Esquema Nacional de Seguridad.

Estrategia de Seguridad de la Dirección General de Informática y Comunicaciones

1. Administración Pública, Sociedad y Seguridad

Nadie tiene dudas sobre la importancia de utilizar los sistemas de información para acercar a los ciudadanos y empresas todos los servicios que la Administración ofrece y debe ofrecer. Esto redunda de manera indiscutible sobre la eficacia, eficiencia y economía, que son principios básicos en la actividad administrativa.

Uno de los mayores cambios que tal vez se han tenido que adoptar desde las Administraciones Públicas ha venido motivado por la llamada Sociedad de la Información, una nueva sociedad que tiene en el uso generalizado de las Nuevas Tecnologías su principal característica. Así, la irrupción de Internet supuso un antes y un después en el funcionamiento y comportamiento de gobiernos, empresas, instituciones y ciudadanos. La llegada y la extensión de la Red de Redes abrió un nuevo mundo de posibilidades de comunicación que transformaba rápidamente las formas de trabajo, relación, compra u ocio de toda la sociedad.

De esta manera, en apenas unos años, las Administraciones Públicas han visto cómo Internet propiciaba un nuevo orden social y económico al que adaptarse. En este sentido, asistimos hoy a un proceso de transformación para abordar los nuevos retos y oportunidades que han propiciado las Nuevas Tecnologías.

Por tanto, vivimos actualmente una profunda revisión de la estructura y funcionamiento de las Administraciones Públicas que pretende mejorar sus mecanismos de relación y comunicación con el ciudadano evolucionando hacia un modelo más proactivo y centrado en las necesidades del CIUDADANO.

El ciudadano quiere encontrar una Administración Pública abierta, que ofrezca un único punto de acceso desde el cual obtener toda la información y realizar los trámites que necesite, de forma clara, sencilla, rápida y segura. Para ello la Administración Pública persigue en la actualidad una simplificación de su funcionamiento, una apuesta clara por la calidad de sus servicios y su centralización, y una mayor sencillez en su relación con la sociedad.

Para alcanzar este escenario, la Administración Pública debe, en primer lugar, mejorar su propio funcionamiento, reorganizando y optimizando sus procesos internos. EN segundo lugar, debe abordar la mejora de la relación e interconexión de los diferentes organismos que conforman la Administración, haciendo más efectivo compartir e intercambiar recursos e información entre ellos.

Para ello, la introducción de Nuevas Tecnologías es un elemento clave.

Banda ancha, soluciones de almacenamiento, redes de comunicaciones IP, herramientas para la gestión administrativa son sólo algunos de los instrumentos que las TICs ponen al alcance de la Administración Pública en su transformación.

La Administración Pública por su parte se encuentra con al menos dos tipos de "clientes":

- aquellos que ya están inmersos en esta Sociedad de la Información, que realmente están DEMANDANDO que las Administraciones Públicas evolucionen y proporcionen los canales adecuados de comunicación, que ya son utilizados y están ampliamente extendidos en otros entornos,

- aquellos ciudadanos que todavía no usan las Nuevas Tecnologías como una herramienta facilitadora de las interacciones.

Por otro lado, en recientes encuestas, se ha podido observar que más de la mitad de los internautas españoles, desconfían de las transacciones electrónicas. Es importante que la Administración Pública, como prestadora de servicios, sea capaz de ganarse la CONFIANZA del ciudadano de manera que este sea capaz de percibir los servicios que se ofrecen a través de la tecnología como algo seguro, confiable, que además ofrezca ventajas respecto a una gestión ágil, rápida, con amplia cobertura temporal y que le suponga un autentico ahorro en tiempo y complejidad.

2. Qué, Por qué, Cómo: El Esquema Nacional de Seguridad.

El Esquema Nacional de Seguridad, recientemente publicado, supone sin duda un antes y un después en la concepción de la seguridad en las Administraciones Públicas. En un cierto sentido afianza las distintas iniciativas en esta materia que se estaban poniendo en práctica desde hace tiempo en las diferentes organizaciones, pero en especial, determina un marco y un enfoque común respecto a la seguridad que permitirá establecer sinergias entre las distintas organizaciones y que constituye un pilar básico para la consecución de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, ya que crea un marco seguro y estable que permitirá compartir recursos entre las distintas administraciones.

El Esquema Nacional de Seguridad indica QUE se debe proteger en una organización, POR QUE debe protegerse y COMO hacerlo.

La definición de SEGURIDAD que ofrece el Esquema Nacional de Seguridad es especialmente destacable porque centra claramente los objetivos que se buscan, los elementos a proteger y los aspectos en los que se debe centrar la seguridad. Concretamente se define seguridad como: "La seguridad es la capacidad de las redes o los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes, acciones ilícitas o malintencionadas, que comprometan la disponibilidad, autenticidad,

integridad, confidencialidad y trazabilidad, de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen, o a través de los que realizan acceso".

Así, se centran en los elementos de la organización que deben ser protegidos frente a acciones no deseables, haciendo foco en los puntos que tienen una importancia fundamental para la consecución de los objetivos, y que suponen un bien valioso y difícilmente sustituible. En concreto, se propone que las acciones se centren en:

- los datos, que conforman sin duda el mayor activo de la organización desde el punto de vista de los sistemas de información,

- los propios sistemas que soportan la gestión de estos datos,

- las comunicaciones electrónicas, las redes por las que fluyen datos, transacciones, peticiones,…

- y los servicios electrónicos, como concepto que transciende más allá del de aplicación, y que es en definitiva lo que la organización ofrece a sus usuarios, a los ciudadanos y empresas.

Una vez establecido QUE hay que proteger, la siguiente cuestión a responder es POR QUE hay que hacerlo.

La respuesta es muy clara. Porque el fin último de la Administración Pública es cumplir una serie de objetivos, una serie de competencias que tiene atribuidas, y así ofrecer servicios a los ciudadanos utilizando sistemas de información.

En cuanto al COMO, el Esquema Nacional de Seguridad marca una serie de principios, sobre los que se debe basar la política de seguridad de cualquier Administración Pública, indicando incluso aquellos requisitos que debe incluir la política definida.

Centrando estos aspectos (POR QUÉ, QUÉ y COMO) en lo referido a la Dirección General de Informática y Comunicaciones, se concretarán los temas de seguridad relativos a aquellos aspectos en los que ejerce sus competencias. Estas son las siguientes:

- Planificación Informática;
- Sistemas de Información y Aplicaciones Informáticas Corporativas;
- Diseño y gestión de las Comunicaciones de la Administración Regional, de sus Organismos Autónomos y de los demás entes de derecho público; así como la coordinación de redes y la Administración Electrónica.
- Coordinación de las Unidades Informáticas de las diferentes Consejerías y Organismos Públicos

- Coordinación en materia de telecomunicaciones; contenidos audiovisuales y Sociedad de la Información

La Dirección General de Informática y Comunicaciones, debido a las competencias que se acaban de enumerar, es la responsable de las comunicaciones de voz y datos tanto internas a la Administración Regional, como entre la Administración de la Comunidad Autónoma de la Región de Murcia, y diferentes agentes como son los ciudadanos y empresas, entidades locales y otras administraciones públicas a través de la red SARA.

Adicionalmente, la Dirección General de Informática y Comunicaciones se relaciona, y debe proteger los activos relativos a los siguientes agentes:

- Personal propio. Este grupo de usuarios están distribuidos en diferentes Consejerías y Organismos Autónomos y hacen uso de los sistemas de información corporativo (Gestión de Personal y Nóminas, Gestión Económico, Financiera y Tributaria, Portales de Intranet,…)
- Entidades locales. A diferentes ayuntamientos se le ofrecen servicios que apoyan el desarrollo de sus propias competencias.
- Ciudadanos y empresas. Portales corporativos de la CARM, servicios de la e-administración, etcétera

Para poder llevar a cabo todo lo indicado anteriormente, se debe establecer una Política de seguridad explicita, pública, que es aprobada y apoyada por el órgano superior competente.

Esta política debe ser coherente dentro de toda la organización, abarcando un conjunto amplio de elementos dentro de la misma (personal, sistemas, servicios,…). Esta política de seguridad se desarrolla definiendo acciones integrales que abarquen diferentes áreas, entretejiendo un sistema robusto y sostenible, en el que "todos los eslabones de la cadena tengan el mismo nivel de resistencia", evitando así aspecto de la seguridad que no se hayan tenido en cuenta y que supongan un punto débil en la organización.

Tanto la política como las decisiones de seguridad están en consonancia con los principios y requisitos indicados en el Esquema Nacional de Seguridad.

3. Proyectos de incremento de la seguridad y Casos de éxito.

La gestión de la seguridad ha sido desde siempre una preocupación fundamental en la Dirección General de Informática y Comunicaciones, aunque en los últimos años se han incrementado las acciones en esta materia, llevándose a cabo numerosos proyectos en todas sus áreas de competencia, garantizando la seguridad en todos los entornos.

A continuación se presentan algunos casos de éxito, que fueron identificados en el análisis diferencial respecto a la norma ISO-27002 que se realizó, como proyectos que habían influido especialmente a la hora de mejorar la seguridad en la organización. En ellos, ya nos encontramos en

ciclos de mejora.

- **Sistemas de gestión de identidad y accesos**

La implantación de un sistema de gestión de identidad y accesos ha permitido disponer de una homogenización de los datos del usuario en todos los sistemas de la Comunidad Autónoma, así como agilizar y racionalizar el uso de los mismos por parte de los usuarios y de sus responsables. Adicionalmente se consigue un punto unificado (debidamente securizado y replicado) de almacenamiento de credenciales (claves + certificado), que está asociado a la propia estructura organizativa y contra el que se autentifican los usuarios de los sistemas.

Este proyecto se subdivide a la vez en dos:

- DARFE. Utilización masiva del certificado digital por parte de los trabajadores de la CARM.
- IDECOR. Identidad Corporativa

- **Adecuación del CPD:**

Este proyecto lleva continuos ciclos de mejora y auditorias en diversos aspectos, como son: el aumento de la disponibilidad a través de actuaciones en el entorno físico donde se encuentran las máquinas (actuaciones en electricidad –SAI, generadores,…-, aire acondicionado, detección de incendios, de humedad,…); Control de accesos y controles de presencia; definición e implantación de los servicios de Housing y Hosting que se ofrecen a otras Unidades Administrativas.

- **ASA.- Arquitectura Avanzada de Seguridad.**

El objetivo principal de este proyecto es la implantación de mecanismos que mejoren la seguridad en las comunicaciones corporativas, tanto frente a Internet y el resto de redes públicas y privadas, así como frente a usuarios internos. Para conseguir esto se cuenta con una doble corona de cortafuegos e incluso en la zona dentro de la capa más interna de esta arquitectura hay una segregación de las redes de servidores y control del trafico.

Entre las políticas de control de redes, también se lleva a cabo el control de tráfico dentro de los edificios para conseguir reducir el riesgo en caso de que algún equipo de usuario se viera comprometido.

Actualmente, nuevas prestaciones derivadas de implantación de soluciones tecnológicas avanzadas (como virtualización de servidores) y el uso intensivo de los servicios de hosting y housing por parte de otras unidades administrativas ha llevado a la puesta en marcha de un ciclo de mejora que de respuesta ágil y sostenible a estas nuevas demandas.

- **Almacenamiento crítico.**

La dato es sin lugar a duda uno de los principales activos de cualquier organización. Su seguridad, entendida en un amplio sentido, debe ser una de las principales preocupaciones de los responsables de los sistemas de información.

Con el fin de garantizar la buena gestión de los datos se procedió a realizar una clasificación y categorización de los distintos datos almacenados y de los sistemas que los soportaban, con el fin de optimizar el almacenamiento respecto a los requisitos de disponibilidad, tiempo de máximo de recuperación, ventana máxima de indisponibilidad. Se creó un sistema de SAN con replicación síncrona en dos ubicaciones distintas con el fin de contener los datos identificados como más críticos para el negocio. Adicionalmente se revisaron y reorganizaron los sistemas de copia de seguridad.

- **Redefinición de las políticas de Internet y Extranet.**

Actualmente es imposible concebir una organización "aislada" de la Red. La seguridad perimetral, y la definición de las distintas formas de interacción entre elementos de la propia organización y actores externos constituye un aspecto de tal importancia, que el esfuerzo de planificación, definición, implantación y control que se requiere se ve rápidamente compensado. Dentro de las actuaciones de seguridad llevadas a cabo, se realizó una redefinición de las políticas de Internet y Extranet, dentro de las cuales cabe destacar:

  - Acceso al correo electrónico de la CARM por parte de los empleados utilizando las mismas garantías de acceso desde Internet y desde Intranet.
  - Acceso puntual por VPN para casos excepcionales, a aplicativos concretos.
  - Acceso a Intranet desde Internet solo a usuarios autorizados y mediante uso de conexiones seguras y certificado digital.
  - Generalización del uso de conexiones encriptadas y certificado digital en los servicios puestos a disposición de los ciudadanos en Internet.

- **Segregación de entornos de aplicaciones.**

En nuestra organización se utilizan entornos totalmente separados para desarrollo, pruebas y producción en todos los entornos. En aquellos aplicativos que no son propios los entornos mínimos son pruebas y producción. Los flujos de traspaso de aplicativos y datos entre entornos entran fuertemente protocolizados y en el caso de tratarse de colecciones de datos de pruebas tomadas desde entornos de producción hacia los de pruebas, se aplica un enmascaramiento de los datos con el fin de realizar totalmente la disociación de los mismos.

4. Líneas estratégicas de seguridad en la Dirección General de

Informática y Comunicaciones

La Dirección General de Informática y Comunicaciones, como ya se ha indicado, tiene atribuidas las competencias en materia de Sistemas de Información y Aplicaciones Informáticas Corporativas.

Con el fin de diseñar una estrategia de gestión de la seguridad se realizaron diversas actuaciones:

- **Análisis diferencial de la norma ISO 27002.** Se hizo un análisis de la situación en un momento concreto de los elementos sobre los que es competente la DGIC (que ya han sido mencionados anteriormente) para poder identificar el grado de madurez, respecto a la seguridad, en el que se encontraban los distintos elementos organizativos.

  Este proyecto resultó especialmente interesante, pues ofreció una visión muy clara de puntos fuertes y débiles, se pudieron identificar proyectos concretos a llevar a cabo, y la prioridad que debían tener de los mismos.

- **Test de intrusión contra sistemas visibles de la organización desde Internet.** Se contrató un hacking ético con una empresa externa, para comprobar las vulnerabilidades que se podían encontrar en un conjunto determinado de nuestros sistemas, y hasta que punto estaban expuestos a ataques internos y externos. Un punto muy interesante de este proyecto consistió en que los agentes encargados de los sistemas no fueron informados de la fecha en la que se producirían los mismos y se pudo también comprobar las medidas de detección, reacción, etc.

Después de analizar las conclusiones de estos trabajos, se establecieron diversas líneas estratégicas y se afianzó el Plan Estratégico de Seguridad. Este Plan pretende establecer un proceso continuo en materia de seguridad que nos sitúe, con la ayuda de nuestros socios tecnológicos, en una posición envidiable en materia de seguridad.

En la Dirección General de Informática y Comunicaciones, se ha basado conjunto de actuaciones de seguridad en la familia de normas ISO-27000 y se han marcado diversas líneas de actuación.

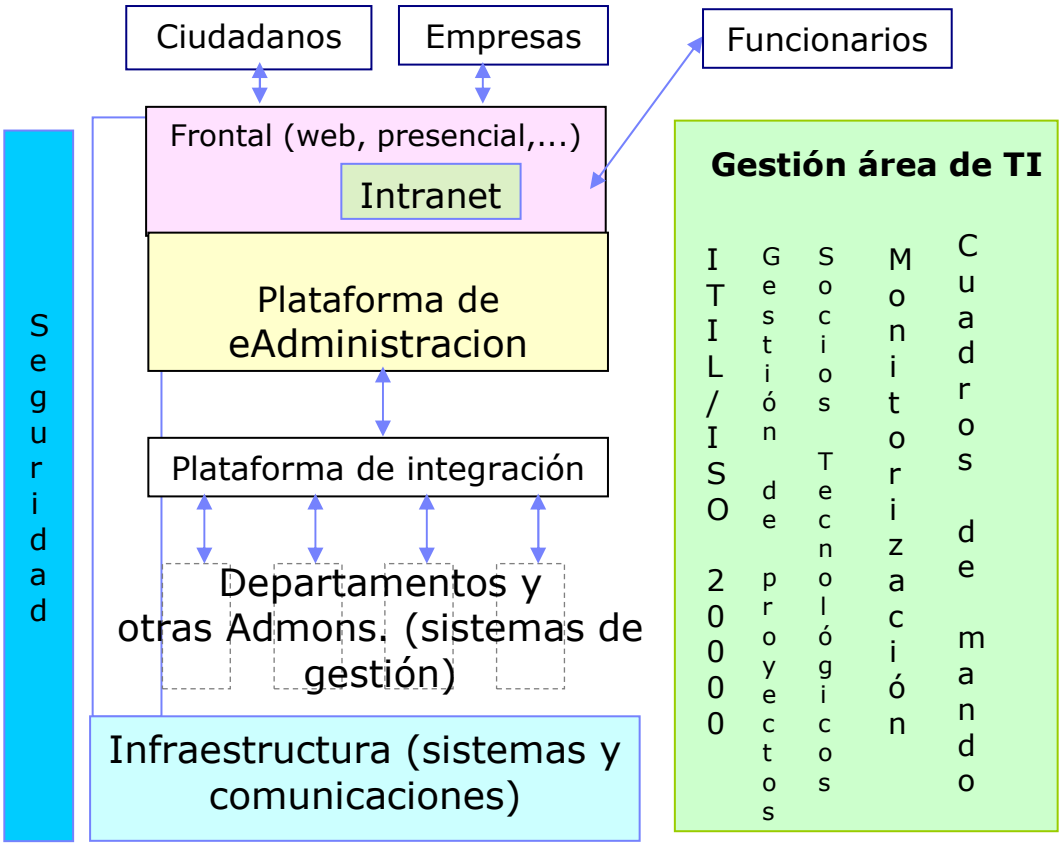
- **Creación de un área de seguridad con competencias propias**

La seguridad se ha sido perfilando como uno de los aspectos ha tener muy en cuenta en nuestra organización. La conciencia e implicación sobre esta materia, ha calado profundamente en toda la estructura, de forma que desde la Dirección se ha decidido dar un fuerte apoyo a la seguridad como parte de la estructura administrativa y que se convierta así en un eje fundamental, transversal a la organización, que aúne los esfuerzos y de una mayor coherencia a las actividades.

Así, se ha creado una estructura estable y diferenciada dentro de la Dirección General, de manera que se pueda concebir la seguridad como una

actividad integral, en la cual la actuaciones son coordinadas desde un mismo lugar, y no dependen de los recursos en cada una de las áreas, sino de un Plan Director en materia de seguridad, que va dotando a la organización de una mejora conjunta y evita de esta manera dejar áreas más vulnerables que otras, cuestión que traería sin duda una debilidad a todo el sistema.

Como se ve en el esquema siguiente, los procesos de seguridad se consideran transversales, respecto a la estructura de la organización.



El destinar un grupo de personas a tareas exclusivas de seguridad, permite una implantación más eficaz de las políticas, protocolos y normas de seguridad, pues se segregan las tareas de definición, implantación y auditoría de las mismas.

Las competencias que se han asignado a esta unidad organizativa son:

- Analizar y estudiar los riesgos sobre los sistemas de información corporativos y planificar y diseñar estrategias para su control.

- Definir políticas, normas y controles de seguridad, pudiendo auditar su

cumplimiento y dictar medidas correctivas en caso de no darse este.

- Planificar, implantar y administrar los sistemas específicos para la seguridad de los sistemas de información.

- Realizar una labor preventiva y de concienciación para la seguridad de los sistemas de información, y gestionar los incidentes que pudieran producirse.

- **Revisión de la política corporativa de seguridad de la información.** Se observaron nuevos elementos que debían ser incorporados a la política de seguridad corporativa, así como a otras políticas de seguridad sobre elementos más concretos que emanan de ella. Actualmente se está en fase de difusión.
- **Formación sobre la necesidad de utilizar las medidas de seguridad.** Se pudo comprobar que después de la formación los usuarios aceptan mejor el uso de las medidas de seguridad.
- **Creación de un SGSI.** Se plantean una serie de actuaciones para crear el Sistema de Gestión de Seguridad de la información (SGSI), según las indicaciones de la ISO-27001, que permita en nuestra organización el diseño, implantación, y especialmente, el mantenimiento de los procesos que permitan gestionar eficientemente la seguridad de la información, minimizando los riesgos. La certificación en la ISO-27001, en nuestro caso no se considera como un fin, sino como una parte del camino para una buena gestión de la seguridad de la información que ha de ser custodiada. Para la gestión automática se utiliza la herramienta SGSI de la empresa Écija.
- **Continuidad de negocio.** Este proyecto está aunando los planes de continuidad previamente existentes para los distintos servicios, sistemas, etc., para unificar criterios y realizar un plan conjunto y general de la organización
- **Seguridad basada en gestión de riesgos.** En el acercamiento a la seguridad basado en gestión de riesgos y en la mejora continua de los procesos, se han priorizado dos tipos de actuaciones. Por un lado la implantación de mejora de aquellos procesos inexistentes en un nivel de madurez bajo, y por otro, la mejora continua de los procesos que se encontraban ya en un nivel de madurez adecuado, con el fin de no "descuidar los puntos fuertes" y aprovechar al máximo el "Know-how" ya existente en la organización.
- **Creación de un CERT.** Actualmente se están realizando ya actuaciones de alerta temprana y ante incidentes informáticos, pero la mayor parte de las veces se producen de manera "reactiva". Se quiere profundizar en el área estableciendo servicios y protocolos adecuados para poder realizar actuaciones reactivas y proactivas respecto a la seguridad y poder extenderlas a toda la organización

Esta Dirección General se ha planteado que la seguridad no es un freno

sino un elemento dinamizador de los procesos, un acicate para hacer las cosas mejor y más rápido. Como se puede observar, las líneas estratégicas marcadas dentro de la Dirección General están perfectamente alineadas con los principios del Esquema Nacional de Seguridad.

5.- Conclusiones

En el momento actual, la innovación en los sistemas de información es un "cambio cultural" que va impregnando a la sociedad y su manera de relacionarse. Las Administraciones Públicas tienen la obligación de servir como impulsoras de esta corriente modernizadora que permitirá a los ciudadanos disfrutar de los servicios a los que tienen derecho, mediante la mayor oferta de canales que las organizaciones sean capaces de poner a su disposición.

Un factor estratégico de éxito para el uso intensivo de las Nuevas Tecnologías es que se consiga generar CONFIANZA en la utilización de los nuevos sistemas y para ello hay que invertir en SEGURIDAD.

Los esfuerzos en seguridad deben ser coordinados desde un punto único en la organización para que las medidas ganen en eficacia, efectividad y coherencia. Así, se deben crear unidades organizativas especializadas con el fin de segregar claramente las distintas responsabilidades sobre los sistemas de información, incrementar la especialización de los profesionales encargados de esta tarea y garantizar una estabilidad temporal en las actuaciones, permitiendo de esta manera conseguir que la organización vaya incrementando sus niveles de seguridad de una manera armónica, alcanzando mayores cotas de madurez en los procesos mediante actividades de mejora continua.

Por último es importante destacar que desde la Dirección General de Informática y Comunicaciones se apuesta por un modelo de seguridad en el que haya una concienciación de todos los agentes implicados en la misma y en el que se fomente la participación de todas las personas de la organización, porque se considera que es la única manera de conseguir la eficacia en los procesos y medidas que garanticen la seguridad.