Política de seguridad de la Información

Esquema Nacional de Seguridad

Fecha: 09/01/2024

Versión 4

1. Aprobación y entrada en vigor

Esta Política de Seguridad de la Información es efectiva desde la fecha de firma y hasta que sea reemplazada por una nueva Política. Dicha Política se revisará cuando proceda, pero al menos una vez al año se realizará esta revisión especificándose en el Informe de la Revisión por la Dirección.

2. Misión de la organización

La Misión de Contazara es:

> *"Aportar valor a los grupos de interés en la gestión del agua y gas con soluciones innovadoras y competitivas mediante una gestión excelente".*

Contazara, siendo consciente de la importancia de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos y asumiendo su compromiso con la seguridad de la información, somete a la adecuada de los mismos, con el fin de ofrecer a todos sus grupos de interés las mayores garantías en torno a la seguridad de la información utilizada.

Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica

que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Los departamentos deben estar preparados para prevenir, vigilar, detectar, reaccionar y recuperarse de incidentes, de acuerdo con el Artículo 8 del ENS (Artículo 8. Prevención, detección, respuesta y conservación. Real Decreto 311/2022, de 3 de mayo de 2022, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Actualizado el 30/03/2021).

Alcance

Esta política se aplica a todos los sistemas TIC de la entidad y a todos los miembros de la organización, implicados en Servicios y Proyectos destinados al sector público, que requieran la aplicación de ENS, sin excepciones.

Objetivos

Por todo lo anteriormente expuesto, la Dirección establece los siguientes objetivos de seguridad de la información para ENS:

- Asegurar la recuperación rápida y eficiente de los servicios, frente a cualquier desastre físico o contingencia que pudiera ocurrir y que pusiera en riesgo la continuidad de las operaciones.

Þ Prevenir incidentes de seguridad de la información en la medida que sea técnica y económicamente viable, así como mitigar los riesgos de seguridad de la información generados por nuestras actividades.

Þ Mejorar la gestión de incidencias en el área de tecnologías de la información y en la gestión de los servicios de telelectura, incluido el área de soporte técnico a cliente.

Þ Mejorar la monitorización de los servicios utilizando herramientas que de forma automática favorezca este seguimiento.

Þ Asegurar la seguridad de las plataformas de telelectura y del sistema propio de Contazara afectado por este aplicativo.

Þ Asegurar la monitorización de log´s del software de los servicios de telelectura y del sistema propio de Contazara.

Þ Garantizar la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información

Marco normativo

Uno de los objetivos debe ser el de cumplir con requisitos legales aplicables y con cualesquiera otros requisitos que suscribimos además de los compromisos adquiridos con los clientes, así como la actualización continua de los mismos. Para ello, el marco legal y regulatorio en el que desarrollamos nuestras actividades es:

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

- Real Decreto Legislativo 1/1996, de 12 de abril, Ley de Propiedad Intelectual.

- Ley 2/2019, de 1 de marzo, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, y por el que se incorporan al ordenamiento jurídico español la Directiva 2014/26/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, y la Directiva (UE) 2017/1564 del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017.

- Real Decreto 311/2022, de 3 de mayo, de desarrollo del Esquema Nacional de Seguridad modificado por el Real Decreto 951/2015, de 23 de octubre.

- Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y de Comercio Electrónico.

- Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

- Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.

- UNE-EN ISO/IEC 27001:2017- Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos

- Instrucciones técnicas de Seguridad más relevantes, teniendo en cuenta que no somos administración pública, son:

  - Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

  - Resolución de 27 de marzo de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Auditoría de la Seguridad de los Sistemas de Información.

  - Resolución de 13 de abril de 2018, de la Secretaría de Estado de Función Pública, por la que se aprueba la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad.

Desarrollo

Para poder lograr estos objetivos es necesario:

Mejorar continuamente nuestro sistema de seguridad de la información

Identificar las amenazas potenciales, así como el impacto en las operaciones de negocio que dichas amenazas, caso de materializarse, puedan causar.

Preservar los intereses de sus principales partes interesadas (clientes, accionistas, empleados y proveedores), la reputación, la marca y las actividades de creación de valor.

Trabajar de forma conjunta con nuestros suministradores y subcontratistas con el fin de mejorar la prestación de servicios de TI, la continuidad de los servicios y la seguridad de la información, que repercutan en una mayor eficiencia de nuestra actividad.

Evaluar y garantizar la competencia técnica del personal, así como asegurar la motivación adecuada de éste para su participación en la mejora continua de nuestros procesos, proporcionando la formación y la comunicación interna adecuada para que desarrollen buenas prácticas definidas en el sistema.

Garantizar el correcto estado de las instalaciones y el equipamiento adecuado, de forma tal que estén en correspondencia con la actividad, objetivos y metas de la empresa.

Garantizar un análisis de manera continua de todos los procesos relevantes, estableciéndose las mejoras pertinentes en cada caso, en función de los resultados obtenidos y de los objetivos establecidos.

Disponer de los recursos económicos necesarios para mejorar aspectos como la gestión de incidencias, monitorización de los servicios de forma automática, mejorar la seguridad del aplicativo web y de nuestro propio sistema, monitorización de log´s del software de los servicios de telelectura y de nuestro sistema, entre otros, …

Estructurar nuestro sistema de gestión de forma que sea fácil de comprender. Nuestro sistema de gestión tiene la siguiente estructura:

La gestión documental de nuestro sistema de gestión recae sobre la Directora de Calidad, Medioambiente, Salud y Seguridad, como responsable de la información, la gestión física del mismo recae sobre el Responsable de IT, como responsable del sistema y la coordinación, aprobación y supervisión de la empresa externa subcontratada que desarrolla nuestro aplicativo web y nos subcontrata los servidores en AWS es responsabilidad del Director de Tecnología & IoT, como responsable de seguridad.

Organización de seguridad

La responsabilidad esencial recae sobre la Dirección General de la organización, ya que esta es responsable de organizar las funciones y responsabilidades y de facilitar los recursos adecuados para conseguir los objetivos del ENS. La Dirección deberá proveer evidencia de su compromiso con la seguridad de la información:

- Establecer la Política de Seguridad
- Garantizar que los objetivos de seguridad de la información estén alineados a la dirección estratégica de la organización.
- Establecer roles y responsabilidades.
- Suministrar los recursos necesarios.
- Decidir los criterios para aceptar el riesgo.
- Garantizar que se ejecuten las auditorías internas.
- Llevar a cabo revisiones por la dirección

Por otro lado, la Dirección se apoya en el Comité de Seguridad de ENS, quienes cumplirán la función de impulsar la implementación de la presente Política.

Los roles o funciones de seguridad definidos son:

Función	Deberes y responsabilidades
Responsable de la información (ENS)	-Tomar las decisiones relativas a la información tratada y su protección - Responsabilidad última si ocurre un incidente de confidencialidad, integridad y disponibilidad junto con el Director General

	- Aprobar los niveles de seguridad de la información con ayuda del Responsable de Seguridad y Responsable del servicio - Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad - Responsable de la protección de datos de carácter personal.
Responsable de los servicios (ENS)	-Coordinar la implantación del sistema depende de las responsabilidades de cada servicio -Mejorar el sistema de forma continua - Aprobar los niveles de seguridad de los servicios con ayuda del Responsable de Seguridad y Responsable del servicio.
Responsable de la seguridad (ENS)	-Determinar la idoneidad de las medidas técnicas -Proporcionar la mejor tecnología para el servicio - Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información
Responsable del sistema (ENS)	- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida junto con el Responsable de la información; así como mejorar de forma continua dicho sistema ayudado del Responsable de la Información. - Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo. - Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad. - Tiene la posibilidad de acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión debe ser acordada con los responsables de la información afectada, del servicio afectado y el responsable de la Seguridad, antes de ser ejecutada.

Esta definición de deberes y responsabilidades se completa en los perfiles de puesto y en los documentos del sistema registro de responsables, roles y responsabilidades.

Comité de Seguridad de ENS

El procedimiento para su designación y renovación será la ratificación en el comité de seguridad.

El comité para la gestión y coordinación de la seguridad relacionado con los aspectos que afectan a Esquema Nacional de Seguridad es el órgano con mayor responsabilidad dentro del sistema de gestión de seguridad de la información según el Real decreto 311/2022, de 3 de mayo, de forma que todas las decisiones más importantes relacionadas con la seguridad se acuerdan por este comité.

Los miembros del comité de seguridad de ENS son:

- Responsable de la Información
- Responsable de los Servicios
- Responsable de la Seguridad
- Responsable del Sistema
- Director General, cuando sea necesario

Estos miembros son designados por el comité, único órgano que puede nombrarlos, renovarlos y cesarlos.

El comité de seguridad es un órgano autónomo, ejecutivo y con autonomía para la toma de decisiones y que no tiene que subordinar su actividad a ningún otro elemento de nuestra empresa.

Este Comité de Seguridad de ENS tendrá entre sus funciones:

- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada área.
- Planificar un análisis y evaluación de riesgos, mínimo cada año.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Presupuestar los recursos necesarios.
- Elaborar un plan de formación y de sensibilización junto con el Departamento de RRHH´s.
- Sancionar las medidas de seguridad en el procesamiento de la información.
- Planificar auditorías internas periódicas.
- Supervisar y reportar sobre eventos e incidentes de seguridad.
- Coordinar el proceso de gestión de la continuidad de operaciones de los sistemas de tratamiento de la información frente a interrupciones imprevistas.

Dicho Comité se reunirá con una periodicidad semestral, siempre y cuando no surja algún aspecto relevante que haga reunirse con cierto carácter de urgencia.

Segregación de funciones y tareas

Toda tarea en la que nuestro personal y/o colaboradores y/o clientes tengan acceso a la infraestructura tecnológica y a los Sistemas de Información, deberá contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso o modificaciones no autorizados sobre los activos de información.

La gestión o ejecución de ciertas tareas o áreas de responsabilidad se separarán a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios, por falta de independencia en la ejecución de funciones críticas.

Gestión de Riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se revisa regularmente:

- Al menos una vez al año;
- Cuando cambie la información manejada;
- Cuando cambien los servicios prestados;
- Cuando ocurra un incidente grave de seguridad;
- Cuando se reporten vulnerabilidades graves.

Para la armonización de los análisis de riesgos, el Comité de Seguridad de ENS establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El Comité de Seguridad de ENS dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

Para la realización del análisis de riesgos se tendrá en cuenta la metodología de análisis de riesgos desarrollada en el procedimiento Análisis de Riesgos.

Respecto a los riesgos derivados del tratamiento de datos personales, se analizan y evalúan como el resto de riesgos afectados por el alcance de Esquema Nacional de Seguridad, como se especifica en el procedimiento de Análisis de Riesgos. Además dicha información con datos de carácter personal se han tenido en cuenta en la categorización del sistema y este flujo de datos de carácter personal es

especificado en el Registro de actividades de tratamiento (RAT), cuya responsabilidad es del Responsable de la protección de datos de carácter personal.

Gestión de Personal

Todos los miembros de Nuestra Organización tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad de ENS disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de nuestra Organización atenderán a una sesión de concienciación en materia de seguridad ENS al menos una vez al año. Se establecerá un programa de concienciación continua para atender a todos los miembros de la organización, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Profesionalidad y seguridad de los recursos humanos

Esta Política se aplica a todo el personal de la organización dentro del alcance de ENS y el personal externo que realiza tareas dentro de la empresa que afecte ENS.

El área de RRHH junto con el Responsable de la Información incluirá funciones de seguridad de la información relacionadas con ENS en las descripciones de los trabajos de los empleados, informará a todo el personal que contrate sus obligaciones con respecto al cumplimiento de la Política de

Seguridad de la Información, gestionará los compromisos de confidencialidad con el personal y coordinará las tareas de capacitación de los usuarios con respecto a esta Política.

El responsable del sistema, es responsable de monitorear, documentar y analizar los incidentes de seguridad reportados, así como de comunicarse al Comité de Seguridad de ENS y a los propietarios de información.

El Comité de Seguridad de ENS será responsable de implementar los medios y canales necesarios para que el responsable del sistema maneje informes de incidentes y anomalías del sistema. El Comité también estará al tanto, supervisará la investigación, supervisará la evolución de la información y promoverá la resolución de incidentes de seguridad de la información.

El Responsable de la Información junto con el Comité de Seguridad de ENS participará en la preparación del Compromiso de Confidencialidad que firmará los empleados y terceros que desempeñen funciones en la organización, en el asesoramiento sobre las sanciones que se aplicarán por incumplimiento de esta Política y en el tratamiento de incidentes de seguridad de la información.

Todo el personal de la organización es responsable de informar sobre las debilidades e incidentes de seguridad de la información que se detectan oportunamente.

Profesionalidad de los recursos humanos:

- Determinar la competencia necesaria del personal para llevar a cabo el trabajo que afecta a la Seguridad de la Información
- Hay que asegurar que las personas sean competentes sobre la base de la educación, capacitación o experiencia adecuadas
- Demostrar mediante la información documentada que sea necesaria la competencia del personal en materia de Seguridad de la Información

Los objetivos de controlar la seguridad del personal son:

- Reducir los riesgos de error humano, puesta en marcha de irregularidades, uso indebido de instalaciones y recursos, y manejo no autorizado de la información.
- Explicar las responsabilidades de seguridad en la etapa de reclutamiento del personal e incluirlas en los acuerdos a firmar y verificar su cumplimiento durante el desempeño de las tareas del empleado.
- Asegúrese de que los usuarios estén al tanto de las amenazas y preocupaciones de seguridad de la información y estén capacitados para apoyar la Política de Seguridad de la Información de la organización en el curso de sus tareas normales.
- Establecer compromisos de confidencialidad con todo el personal y usuarios fuera de las instalaciones de procesamiento de información.
- Establecer las herramientas y mecanismos necesarios para promover la comunicación de las debilidades de seguridad existentes, así como los incidentes, con el fin de minimizar sus efectos y prevenir su reincidencia.

Autorización y control de acceso a los Sistemas de Información

- El control del acceso a los sistemas de información tiene por objetivo:
- Evitar el acceso no autorizado a sistemas de información, bases de datos y servicios de información.
- Implementar la seguridad en el acceso de los usuarios a través de técnicas de autenticación y autorización.
- Controlar la seguridad en la conexión entre la red de la organización y otras redes públicas o privadas.

- Revisar los eventos críticos y las actividades llevadas a cabo por los usuarios en los sistemas.
- Concienciar sobre su responsabilidad por el uso de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utilizan ordenadores portátiles y ordenadores personales para el trabajo remoto.

Protección de las instalaciones

Los objetivos de esta política en materia de protección de las instalaciones son:

- Prevenir el acceso no autorizado, daños e interferencias a la sede, instalaciones e información de nuestra organización.
- Proteger el equipo de procesamiento de información crítico de la organización, colocándolo en áreas protegidas y protegido por un perímetro de seguridad definido, con las medidas de seguridad y controles de acceso adecuados. Asimismo, contemplar la protección de esta en su traslado y permanecer fuera de las áreas protegidas, por mantenimiento u otros motivos.
- Controlar los factores ambientales que podrían perjudicar el buen funcionamiento del equipo de cómputo que alberga la información de la organización.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus tareas habituales.
- Proporcionar protección proporcional a los riesgos identificados.
- Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información de la organización: instalaciones, equipos, cableado, expedientes, medios de almacenamiento, etc.

- El responsable de la información, junto con el responsable de seguridad y el responsable del sistema, según proceda, definirá las medidas de seguridad física y ambiental para la protección de los activos críticos, sobre la base de un análisis de riesgos, y supervisará su aplicación. También verificará el cumplimiento de las disposiciones de seguridad física y medioambiental.

- Los responsables de los diferentes departamentos definirán los niveles de acceso físico del personal de la organización a las áreas restringidas bajo su responsabilidad. Los Propietarios de Información autorizará formalmente el trabajo fuera del sitio con información sobre su negocio a los empleados de la organización cuando lo consideren apropiado.

- Todo el personal de la organización es responsable del cumplimiento de la política de pantalla limpia y escritorio, para la protección de la información relacionada con el trabajo diario en las oficinas.

Adquisición de productos

Los diferentes departamentos deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

Por otro lado, se tendrá en cuenta la seguridad de la información en la adquisición y mantenimiento de los sistemas de información, limitando y gestionando el cambio.

La política de desarrollo y adquisición de sistemas de información se desarrolla en el documento: Instrucción de trabajo 126 Requisitos de compra de IT.

Seguridad por defecto

La organización considera estratégico para la entidad que los procesos integren la seguridad de la información como parte de su ciclo de vida. Los sistemas de información y los servicios deben incluir la seguridad por defecto desde su creación hasta su retirada, incluyéndose la seguridad en las decisiones de desarrollo y/o adquisición y en todas las actividades en explotación estableciéndose la seguridad como un proceso integral y transversal.

Integridad y actualización del sistema

Nuestra Organización se compromete a garantizar la integridad del sistema mediante un proceso de gestión de cambios que permita el control de la actualización de los elementos físicos o lógicos mediante la autorización previa a su instalación en el sistema. Dicha evaluación será llevada a cabo principalmente por la dirección de sistemas y cuando sea necesario por el responsable de seguridad, que evaluará el impacto en la seguridad del sistema antes de realizar los cambios y controlará de forma documentada aquellos cambios que se evalúen como importantes o con implicaciones en la seguridad de los sistemas.

Mediante revisiones periódicas de seguridad se evaluará el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

Calificación de la información

La categorización del sistema se ha tenido en cuenta los criterios de la guía *CCN-STIC 803 Valoración de los sistemas* y se ha registrado dicha categorización en el registro “Categorización del sistema”.

Por otro lado, Contazara clasifica la información entre “confidencial, “uso restringido a proveedor” e “interna”, como se especifica en el procedimiento de “Clasificación de la información”. En dicho procedimiento también se explica cómo se identifica dicha información.

Protección de la información almacenada y en tránsito

La organización establece medidas de protección para la Seguridad de la Información almacenada o en tránsito a través de entornos inseguros. Tendrán la consideración de entornos inseguros los equipos portátiles, móviles y soportes de información. Las medidas de seguridad se especifican sobre todo en la política de activos y en menor medida en la política de PC´s y política de móviles.

Prevención de sistemas de información interconectados

La Organización establece medidas de protección para la Seguridad de la Información especialmente para proteger el perímetro, en particular, si se conecta a redes públicas, especialmente si se utilizan en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público

En todo caso se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión. Conexiones electrónicas disponibles para el público.

Estos sistemas de información interconectados están especificados en el documento de Arquitectura de seguridad.

Registros de actividad

La organización registrará las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Los objetivos principales de la Gestión de incidentes son los de:

- Establecer un sistema de detección y reacción frente a código dañino
- Disponer de procedimientos de gestión de incidentes de seguridad y de debilidades detectadas en los elementos del sistema de información.
- Estos procedimientos cubrirán los mecanismos de detección, los criterios de clasificación, los procedimientos de análisis y resolución, así como los cauces de comunicación a las partes interesadas y el registro de las actuaciones.
- Este registro se emplea para la mejora continua de la seguridad del sistema.
- Garantizar que los servicios de IT vuelvan a tener un desempeño óptimo.
- Reducir los posibles riesgos e impactos que pueda causar el incidente.
- Velar por la integridad de los sistemas en el caso de un incidente de seguridad
- Comunicar el impacto de un incidente tan pronto como se detecte para activar la alarma; y poner en práctica un plan de comunicación empresarial adecuado.
- Promover la eficiencia empresarial.

Todo el proceso de gestión de incidencias está especificado más detenidamente en el procedimiento de incidencias de seguridad de la información (PG42.7) y en el procedimiento de brechas o violaciones de seguridad para datos de carácter personal (PG42.4).

Continuidad de la actividad

La organización con el objetivo de garantizar la continuidad de las actividades establece medidas para que los sistemas dispongan de copias de seguridad y establezcan mecanismos necesarios para garantizar la continuidad de las operaciones, en caso de pérdida de los medios habituales de trabajo.

Mejora continua del proceso de seguridad

La organización establece un proceso de mejora continua de la seguridad de la información aplicando los criterios y metodología establecida.

Aprobado por Dirección. (Fecha 09.01.24 Edición: 4)