1. OBJETO

La información es un recurso que, como el resto de los activos, tiene valor para **CIGESOC** y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la organización.

Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se asegura un compromiso manifiesto de la Dirección de **CIGESOC** y de los directores de cada uno de los departamentos para la difusión, consolidación y cumplimiento de la presente política.

Más allá de cuál sea el criterio aplicado llegaremos a que la Seguridad de la Información tiene como objetivo preservar:

- **CONFIDENCIALIDAD**: la información debe ser accesible sólo a aquellas personas autorizadas a tal fin.
- **INTEGRIDAD**: la información y sus métodos de procesamiento deben ser completos y exactos.
- **DISPONIBILIDAD**: la información y sus recursos relacionados deben estar disponibles cada vez que se los requiera.
- **AUTENTICIDAD**: debemos valorar la importancia que tendría que el activo no fuera auténtico.
- **TRAZABILIDAD**: importancia que tendría que no se pudiera identificar a quien haya ejecutado una acción.

Pero particularmente, con la implantación de esta política de seguridad pretendemos alcanzar los siguientes objetivos:

- Proteger los recursos de información de la organización y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
- El cumplimiento de la legislación y reglamentación aplicable, así como el compromiso de cumplir los requisitos establecidos voluntariamente.
- Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

- Mantener la Política de Seguridad de la organización actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
- Garantizar que el riesgo al que está expuesto **CIGESOC** se mantiene bajo unos niveles aceptables.
- Generar un ambiente de trabajo donde se reconozca y valore la actividad en seguridad desarrollada por el personal. Además, generar una cultura general para la realización de un trabajo seguro y procedimentado que no eleve los niveles de riesgo a los que se expone **CIGESOC**.
- Proporcionar una guía para establecer los estándares, procedimientos y medidas de seguridad para seguir desarrollando un Sistema de Seguridad de la Información en el futuro.

2. ÁMBITO DE APLICACIÓN

Esta Política se aplica en todo el ámbito de la organización, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Más adelante, haremos una descripción detallada del entorno existente en la empresa.

Además, se encuentra a disposición del público que la solicite y es revisada cuando así lo estima necesario.

3. DEFINICIONES

- Confidencialidad: la información debe ser accesible sólo a aquellas personas autorizadas a tal fin.
- Integridad: la información y sus métodos de procesamiento deben ser completos y exactos.
- Disponibilidad: la información y sus recursos relacionados deben estar disponibles cada vez que se los requiera.
- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.
- Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

- Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- Tecnología de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

4. DESARROLLO

4.1. Introducción

4.1.1. Revisión y mejora

El Responsable de Seguridad será el encargado de realizar el adecuado control interno para evaluar la eficacia de los controles implementados y tener actualizados todos los procedimientos y procesos aplicados en la empresa ante posibles cambios de negocio o de requisitos de seguridad.

El Comité de Seguridad, integrado por el Responsable de Seguridad, la Directora Técnica y los administradores de sistemas, realizará una revisión global del sistema, con periodicidad anual, en la que se valore la eficacia del sistema, se revise el cumplimiento de los objetivos fijados y se establezcan nuevos objetivos, coincidente normalmente con la revisión por la dirección.

Para optimizar y mejorar de modo permanente el sistema de gestión de la seguridad de la información, al menos, se tendrán en cuenta las siguientes actividades:

- El registro y seguimiento de no conformidades y reclamaciones.
- El registro y seguimiento de las acciones correctivas
- El registro y seguimiento de las acciones preventivas realizadas.
- Análisis periódico de las mejoras propuestas

En cada ciclo del sistema se plantearán nuevos objetivos de mejora, planificándolos adecuadamente para poder realizar su correspondiente seguimiento.

Para ello, habrá dos tipos de actuaciones:

- Revisión anual del sistema.
- Revisión ocasional ante fallas importantes de seguridad que deban ser subsanadas de inmediato.

4.1.2. Responsables y responsabilidades

Responsable de la Información: El Responsable de la Información es habitualmente una persona situada en el nivel Directivo de la organización.

- Esta figura tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección.
- El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).
- Tiene la potestad de establecer los requisitos de la información en materia de seguridad, es decir, de determinar los niveles de seguridad de la información

Responsable del Sistema de Gestión: La Dirección de **CIGESOC** designa al Responsable del Sistema de Gestión (RSG) quien, independientemente de otras responsabilidades, tiene la responsabilidad y autoridad para:

- asegurar que se establecen, implantan y mantienen los procesos y requisitos necesarios para el SIG;
- informar a la Dirección sobre el desempeño del SIG, y de cualquier necesidad de mejora;
- asegurar que se promueve la toma de conciencia de los requisitos de los clientes en todos los niveles de la organización;
- gestionar las relaciones con partes externas sobre asuntos relacionados con el SIG

Responsable de Seguridad: Es el encargado de coordinar y controlar las medidas definidas en el presente documento. Mas concretamente:

- Valorar si el activo está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.
- Asegurarse de que el software que se utiliza tiene licencia.
- Asegurarse de que el activo cuenta con el mantenimiento adecuado.
- Asegurarse de que los soportes y equipos que contengan información son desechados según lo establecido.
- Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o interrupción en los servicios.
- Mantener documentación actualizada de todas las funciones críticas para asegurar la continuidad de las operaciones en caso de que alguien no esté disponible.
- Definir quiénes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.
- Proporcionar los mecanismos necesarios para que el personal pueda informar inmediatamente de cualquier violación de seguridad o mal uso de la información o los sistemas. El propietario del activo deberá informar a su vez al Responsable de Seguridad para tratar la incidencia.

- Asegurarse de que los empleados cuentan con la formación adecuada, conoce y comprende la Política de Seguridad y pone en práctica las directrices de seguridad.
- En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.
- Informar al Responsable de Seguridad cuando ocurran cambios de personal que afecten al acceso de la información o los sistemas (cambio de función o departamento, causar baja en la empresa) para que se modifiquen apropiadamente los permisos de acceso.

Responsable de Servicios: Será la persona responsable de establecer los requisitos del servicio en materia de seguridad, o, tendrá la potestad de determinar los niveles de seguridad de los servicios.

Comité de Seguridad: integrado por el responsable de seguridad, la Dirección Técnica, la Responsable del Servicio y los administradores de sistemas, realizará una revisión global del sistema, con periodicidad anual, en la que se valore la eficacia del sistema, se revise el cumplimiento de los objetivos fijados y se establezcan nuevos objetivos.

Administradores de Sistemas: son los responsables de realizar las tareas rutinarias que garantizan que los sistemas están protegidos, dentro de las cuales se recogen tanto las tareas y registros motivados por la implantación de la LOPD como los propios derivados de la ISO 27001 y el ENS. Junto con el responsable de seguridad conforman el Comité de Seguridad.

Dirección: De forma concreta, gestiona el control de acceso a la oficina.

4.1.3. Protección del conocimiento

Para evitar la pérdida, robo o transferencia no autorizada de la propiedad intelectual o información clasificada por **CIGESOC**, se seguirán las reglas principales siguientes:

- La identificación y clasificación de toda la información, en cualquier soporte, considerada de especial protección.
- La firma por parte de todos los usuarios de un compromiso de confidencialidad.
- El seguimiento de todos los controles para el acceso, manejo, reproducción de dicha información.
- La monitorización de estos controles.
- El seguimiento de una política de puesto de trabajo despejado de papeles con información relevante y bloqueo de pantalla mediante contraseña cuando el equipo esté desatendido o no esté en uso, para asegurar la protección de información sensible.

4.1.4. Propietarios de la información

Todos los activos de información tendrán un Propietario, asignándole la responsabilidad del mantenimiento de los controles apropiados.

Para garantizar que se realiza una protección eficaz, el RSEG impulsará la realización de un Inventario de Activos. Este proceso es un aspecto muy importante de la Gestión de Riesgos, ya que permite identificar el valor e importancia relativa a cada activo. Este inventario, se puede dividir según los activos asociados con los Sistemas de Información.

Los activos de información serán clasificados de acuerdo con la siguiente escala:

- **Confidencial**: Información a la que sólo determinadas personas o departamentos dentro de la organización deben tener acceso. Si se filtrara a terceras partes, podría tener consecuencias negativas para la organización
- **Uso Interno**: Información a la que sólo debe tener acceso el personal de la organización. Si se filtrara a terceras partes, podría tener consecuencias para la organización.
- **Público**: Información sin ninguna restricción de acceso. Si se filtrara a terceras partes, no tendría consecuencias para la organización

Tanto la autorización de acceso como la transmisión de esta información por cualquier medio necesitan la aprobación expresa del responsable del activo. La destrucción de esta información la realizará el responsable del activo siguiendo las pautas aprobadas por el RSEG y con su colaboración si es necesaria.

4.2. Entorno

A continuación, describimos brevemente el entorno informático de la empresa, lo que incluye aquellos recursos informáticos internos, externos, además del acceso físico a los mismos.

4.2.1. Recursos informáticos internos

Los recursos informáticos existentes en la empresa se pueden clasificar en:

- Dispositivos informáticos de usuario: están formado por el conjunto de ordenador personal o portátil y teléfono móvil del que disponen cada uno de los empleados de TRISON.
- Dispositivos informáticos de servidor: son todos aquellos dispositivos cuyo uso es compartido por todos los terminales de usuario y en los que reside de forma centralizada la información.
- Dispositivos de comunicaciones: incluimos en este capítulo aquellos dispositivos que permiten la comunicación entre terminales, servidores e Internet, tanto para las comunicaciones de datos como de voz.
- Otros dispositivos: se incluyen aquel equipamiento existente en los laboratorios para maquetas y pruebas, además de las impresoras.

4.2.2. Puestos de usuarios

Se ha hecho un esfuerzo por homologar todos los terminales de usuario, definiendo un Terminal tipo como aquel dispositivo que cumple:

- Sistema operativo: MS Windows10
- Plataforma hardware:
    - Portátil (en su mayoría del fabricante Lenovo o HP)
    - Sobremesa (en su mayoría del fabricante HP)
- Aplicaciones:
    - Ofimáticas (MS Office, Libreoffice)
    - Empresariales (ERP),
    - Correo electrónico (Microsoft Outlook),
    - Navegador (Internet Explorer, Google Chrome y/o Firefox)

Aquellos usuarios que, por su trabajo, habitualmente están fuera de la oficina están provistos de un teléfono móvil Smartphone y tiene acceso a Internet y/o correo electrónico corporativo.

Todos los portátiles están dados de alta en el grupo de trabajo Windows existente y es necesario el uso de contraseña para tener acceso al mismo (dentro o fuera de la red interna de **CIGESOC**).

4.2.3. Servidores

Todos estos terminales están organizados en un grupo de trabajo único basado en Microsoft Windows Server, en el que disponemos de los siguientes recursos:

- Controladores de dominio: un servidor en el que reside los servicios de DNS.
- Servidores de almacenamiento: servidor dedicado a almacenamiento en el que residen todos los ficheros con información. Dispone de sistemas raid para la protección física y lógica de la información y de control de acceso. A su vez este dispositivo dispone de un sistema de copias de seguridad para salvaguardar la información ante un desastre mayor.
- Servidores de aplicaciones: en ellos residen las aplicaciones corporativas.
- Servidor correo: Físicamente hay un servidor que puede alojar cualquier servicio (Office 365 y Exchange Online)

4.2.4. Comunicaciones

Se disponen de un conmutador Ethernet para conectar todos los puestos informáticos de los usuarios y servidor.

También se ha dispuesto de varios puntos de acceso wifi para facilitar el acceso a Internet y a la propia empresa.

4.3. Recursos informáticos externos

Dentro de este apartado, cubrimos aquellos servicios públicos que damos desde equipos que no están dentro de la red de **CIGESOC**.

En la actualidad estos servicios se están dando desde Arsys, AWS, Azure, Google, … en una modalidad de hosting compartido por lo que no disponemos de hardware en exclusiva para **CIGESOC**, sino que nos prestan un servicio sobre dispositivos utilizados por otros clientes.

Los servicios prestados son:

- DNS para los dominios
- Servicio de correo (con antivirus y ANTI-SPAM)
- Servicio web: para la web
- Servicio FTP para los dominios
- Servicio de redirección para el resto de los dominios
- Servicios de almacenamiento

4.4. Acceso Físico

Para que una seguridad lógica sea efectiva es primordial que las instalaciones de **CIGESOC** mantengan una correcta seguridad física. Esta seguridad física está destinada a evitar los accesos no autorizados, así como, cualquier otro tipo de daño o interferencia externa. **CIGESOC** tomará las precauciones necesarias para que sólo las personas autorizadas tengan acceso a las instalaciones.

La oficina cuenta con las barreras físicas necesarias para asegurar los recursos que éstas albergan. Los armarios de comunicaciones donde se ubican los servidores y el cableado estarán cerrados bajo llave y sólo tendrán acceso las personas autorizadas y los terceros cuando vayan acompañados por alguien autorizado.

Las instalaciones están dotadas de dispositivos de extinción de incendios marcados por la legislación vigente en esa materia. En este sentido, se dispone de extintores y salidas de emergencia debidamente señalizados.

Los equipos deberán mantenerse de forma adecuada para garantizar su correcto funcionamiento y su perfecto estado, de forma que mantengan la confidencialidad, integridad y la disponibilidad de la información. Para ello, deben someterse a las revisiones recomendadas por el suministrador. Sólo el personal debidamente autorizado podrá acceder al equipo para proceder a su reparación.

La eliminación de equipos sólo se llevará a cabo por el Responsable de Seguridad o personal en el que éste delegue.

4.5. Política de uso aceptable de los recursos.

Las siguientes actividades están, en general, prohibidas. Los empleados puedes estar excluidos de esta prohibición temporalmente para la realización legítima de las responsabilidades de su trabajo (p.e., administradores de sistemas pueden tener la necesidad de impedir el acceso a la red a un ordenador que se considera está provocando problemas, ha sido comprometido, …).

En ninguna circunstancia, ningún empleado de **CIGESOC**, está autorizado para realizar alguna actividad ilegal (bajo cualquier legislación de cualquier ámbito sea este local, regional, nacional o internacional) con los recursos que la empresa pone a su disposición.

La siguiente lista no pretende ser exhaustiva, sino que intenta servir de guía de actividades que caen dentro de la categoría de uso no aceptable.

Actividades de Red y/o Sistemas

- Violaciones de los derechos de cualquier persona o compañía protegidos por copyright, patente o cualquier tipo de propiedad intelectual, legislación y/o regulación existente, incluyendo (y sin limitarse sólo a esto) la instalación y/o distribución de software pirata o no licenciado para su uso por parte de CIGESOC.
- Copia no autorizada, incluyendo fotocopia, digitalización, … y posterior distribución de cualquier documento (revistas, libros, música…) o fuente con copyright.
- Introducción de programas, scripts o cualquier tipo de software malicioso en los servidores, ordenadores, dispositivos de red, … (virus, worms, Trojan horses, e-mail bombs, etc.).
- Revelar la contraseña a otros. Esto incluye familiares y cualquier otra personal que pueda acceder desde cualquier ubicación externa a la empresa.
- Utilizar los medios que CIGESOC pone a su disposición para conseguir y/o transmitir material que viola las leyes de acoso sexual o abuso en el trabajo de cualquier tipo.
- Realizar ofertas fraudulentas de productos, artículos o servicios.
- Provocar problemas o pérdidas en el nivel de seguridad y/o caídas en las comunicaciones. Por problemas de seguridad también se entiende el acceso a información que no está dirigida a otros, utilizar cuentas para las que no se está autorizado (aunque se conozcan sus credenciales), acceder a ordenadores a los que no se tiene autorización, interceptar cualquier tipo de información de otros (especialmente claves), ... Caídas o mermas de las comunicaciones incluyen actividades como capturas de tráfico, ping floods, spoofing, ataques de denegación de servicio (sea esta parcial o total), falsear información de routing, port or security scanning, …

- Utilizar programas, scripts, comandos, … o enviar mensajes de cualquier tipo con la intención de interferir o deshabilitar una sesión de un usuario en cualquier sentido, localmente o vía Internet, intranet, extranet.
- Proporcionar información o listas de los empleados de CIGESOC a cualquier grupo externo a la empresa.

Actividades de comunicaciones o correo electrónico

- Enviar mensajes de correo no solicitados, incluyendo "junk email" (varios correos casi idénticos enviados a múltiples destinos) o cualquier otro material publicitario a personas que no han solicitado dichos mensajes.
- Cualquier forma de acoso vía correo electrónico, teléfono, sms, … bien sea por el estilo del lenguaje, la frecuencia o el tamaño de los mensajes.
- Uso no autorizado o manipulación de la información de las cabeceras del correo.
- Solicitar correos de cualquier otra fuente distinta al destinatario con la intención de recopilar respuestas.
- Crear o reenviar "cartas en cadena", utilizar esquemas piramidales u otros sistemas similares.
- Envío de correos iguales o similares a grandes cantidades de grupos (listas de distribución, redes sociales, usenet newsgroups, …)

5. CONTROL DE CAMBIOS Y MODIFICACIONES

Fecha	Edición	Naturaleza del Cambio
30/06/2020	01	Primer ejemplar
10/01/2021	02	Revisión funciones y responsabilidades