NORMA DE SEGURIDAD DE LAS TIC
(CCN-STIC-204)

ESTRUCTURA Y CONTENIDO DEL DOCUMENTO ABREVIADO CO/DRES/POS PARA ESTACIONES DE TRABAJO AISLADAS Y PEQUEÑAS REDES

MARZO 2008

Edita:

NIPO: 076-07-236-6

Tirada: 1000 ejemplares
Fecha de Edición: diciembre de 2007
ISDEFE S.A. ha participado en la elaboración y modificación del presente documento y sus anexos

PRÓLOGO

Entre los elementos más característicos del actual escenario nacional e internacional figura el desarrollo alcanzado por las Tecnologías de la Información y las Comunicaciones (TIC), así como los riesgos emergentes asociados a su utilización. La Administración no es ajena a este escenario, y el desarrollo, adquisición, conservación y utilización segura de las TIC por parte de la Administración es necesario para garantizar su funcionamiento eficaz al servicio del ciudadano y de los intereses nacionales.

Partiendo del conocimiento y la experiencia del Centro sobre amenazas y vulnerabilidades en materia de riesgos emergentes, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Una de las funciones más destacables que, asigna al mismo, el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración.

La serie de documentos CCN-STIC se ha elaborado para dar cumplimiento a esta función, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Marzo de 2008

Alberto Sáiz
Secretario de Estado
Director del Centro Criptológico Nacional

1. INTRODUCCIÓN

1. En el Procedimiento de Acreditación Nacional se establece la obligatoriedad de someter a todos los Sistemas de las Tecnologías de la Información y las Comunicaciones (en adelante, Sistemas) que manejen información clasificada a un proceso de acreditación, previo a la concesión de la autorización para manejar dicha información.

2. Asimismo, se define el proceso a seguir, la documentación necesaria y las características mínimas de seguridad que deben cumplir dichos Sistemas para que puedan ser acreditados por la Autoridad correspondiente.

3. La complejidad de la elaboración de la documentación de seguridad aconseja prever el caso de Sistemas sencillos. Para Sistemas formados por estaciones de trabajo o pequeñas redes (1 servidor y 10 estaciones de trabajo como máximo), aisladas o con interconexión hacia el exterior, la redacción de los documentos puede simplificarse siempre que se especifiquen todos los requisitos contemplados en el Procedimiento de Acreditación.

2. OBJETO

4. Definir, en apoyo al Procedimiento de Acreditación Nacional, la estructura y el contenido del documento abreviado CO/DRES/POS para los Sistemas que manejen información clasificada, formados por estaciones de trabajo aisladas o por pequeñas redes, según lo establecido en la política STIC para la Administración.

3. ALCANCE

5. Esta norma será de aplicación para aquellos Sistemas, aislados o con interconexión hacia el exterior, que necesiten manejar información clasificada hasta un grado máximo de clasificación de RESERVADO o equivalente, y que estén configurados como un único nodo compuesto por un máximo de un servidor y diez (10) estaciones de trabajo, ubicado en su conjunto dentro del mismo Entorno Global de Seguridad y trabajando en el modo seguro de operación Unificado al Nivel Superior.

6. Cuando el Sistema disponga de interconexión, para la acreditación de la misma deberá cumplirse lo establecido en la Instrucción Técnica CCN-STIC-302 y redactar, además del documento abreviado CO/DRES/POS, la correspondiente DRSI.

7. Este documento será de aplicación, a criterio de la Autoridad correspondiente, en Sistemas que manejen otro tipo de información en la Administración.

4. DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA

8. Todo Sistema que maneje información clasificada debe disponer de una documentación de seguridad según lo establecido en el Procedimiento CCN-STIC-101.

9. Para las redes pequeñas operando en modo Unificado a Nivel Superior, el Concepto de Operación (CO) y la Declaración de Requisitos Específicos de Seguridad (DRES) se podrán refundir en un único documento abreviado a cumplimentar por la Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones (AOSTIC).

10. El documento abreviado, o parte del mismo, con la inclusión de los anexos que considere necesarios la AOSTIC podrá constituir los Procedimientos Operativos de Seguridad (POS) que deberán ser conocidos por todos los usuarios del Sistema.

11. Para solicitar la correspondiente acreditación, una vez instalado y configurado el Sistema, la AOSTIC deberá remitir el documento abreviado cumplimentado a la Autoridad de Acreditación correspondiente.

12. En el anexo se recoge un ejemplo de aplicación del documento abreviado CO/DRES/POS, que puede ser modificado por los responsables de seguridad de un Sistema, pero que en cualquier caso, debe ser validado por la Autoridad responsable de la acreditación.

5. REDACCIÓN, VALIDACIÓN Y DISTRIBUCIÓN

13. La AOSTIC elaborará el documento abreviado CO/DRES/POS del Sistema.

14. El documento abreviado CO/DRES/POS deberá ser validado por la Autoridad responsable de acreditar el Sistema, como parte del proceso de acreditación para Sistemas que manejen información Nacional/OTAN/UE/ESA clasificada en la Administración.

15. Será necesario asignar al documento abreviado la clasificación apropiada de acuerdo a la información que contiene.

16. Todos los usuarios del Sistema deberán conocer la parte correspondiente a los POS o aquellas partes de los mismos que les sean de aplicación.

17. La AOSTIC, o en quién ésta delegue, deberá exigir un documento de conformidad y aceptación de los POS para cada usuario del Sistema.

6. CONTENIDO DEL DOCUMENTO ABREVIADO CO/DRES/POS

18. Se deberán incluir las siguientes secciones cuando sean pertinentes al Sistema concreto:
    - Sección 1: Solicitud y Organización de Seguridad
    - Sección 2: Concepto de Operación
    - Sección 3: Diagrama de la red con el direccionamiento
    - Sección 4: Configuración Hardware del Sistema
    - Sección 5: Configuración Software del Sistema
    - Sección 6: Servicios Proporcionados por el Sistema
    - Sección 7: Protocolos y puertos habilitados
    - Sección 8: Seguridad de las TIC
    - Sección 9: Gestión de la seguridad de las TIC
    - Sección 10: Seguridad Física
    - Sección 11: Seguridad en el Personal
    - Sección 12: Seguridad Documental
    - Anexos

19. Si se considera necesario, cada una de las secciones puede tomarse aisladamente y utilizarse como un documento independiente para grupos concretos de usuarios o administradores.

20. Las siguientes directrices tienen como fin proporcionar el conjunto de los aspectos de seguridad a considerar en un Sistema genérico. Por tanto, el contenido de cada sección variará dependiendo del Sistema considerado, debiendo ser adaptado a cada Sistema en concreto. Deberá consultarse a la Autoridad responsable de acreditar el Sistema cuando se necesiten solucionar temas de aplicación y de detalle de los POS.

21. Cuando sea necesario incluir información extraída de otros documentos de seguridad del Sistema, puede ser recomendable hacer referencia al documento que la contiene en lugar de incluir la propia información en el documento. Esto permitirá evitar duplicidades y posibles problemas de incoherencia.

6.1. SECCIÓN 1. SOLICITUD Y ORGANIZACIÓN DE SEGURIDAD

22. Esta sección deberá recoger los datos de la solicitud de acreditación del Sistema considerado, y la organización o estructura de seguridad. Para la definición de la estructura de seguridad se podrá emplear la Guía CCN-STIC-402 adaptada a cada caso concreto.

23. Como anexo al documento abreviado se incluirá una lista de usuarios autorizados.

6.2. SECCIÓN 2. CONCEPTO DE OPERACIÓN

24. Esta sección deberá recoger los datos relativos al Concepto de Operación del Sistema:
    - Objeto o función asignada al Sistema.
    - Composición del Sistema.
    - Grado de clasificación de la información a manejar y el modo seguro de operación.
    - Amenazas.
    - Documentación de referencia: documentación común de aplicación al nodo, como una Declaración de Requisitos Específicos de Seguridad Comunes (DRESC).

6.3. SECCIÓN 3. DIAGRAMA DE LA RED CON DIRECCIONAMIENTO

25. Deberá incluirse un diagrama de la red, en el que quede reflejado la arquitectura de la misma, así como su direccionamiento.

6.4. SECCIÓN 4. CONFIGURACIÓN HARDWARE DEL SISTEMA

26. Deberán incluirse, cuando sean de aplicación, los siguientes datos:
    - Características hardware del servidor y/o de las estaciones de trabajo: marca/modelo, microprocesador, memoria RAM, disco duro, periféricos, monitor, teclado/ratón, y cualquier otra información que se considere de interés.
    - Dispositivos de comunicaciones y periféricos del Sistema: router (Marca/Modelo), switch, cifrador, impresoras, escáner, etc.

6.5. SECCIÓN 5. CONFIGURACIÓN SOFTWARE DEL SISTEMA

27. Deberá incluirse, cuando sean de aplicación, los siguientes datos:
    - Características del software del servidor y/o de las estaciones de trabajo: sistema operativo (incluyendo la versión y actualizaciones), servicios habilitados,...
    - Herramientas de seguridad: detección de SW dañino, borrado seguro, análisis de vulnerabilidades, etc. Para ello se podrá emplear la Instrucción Técnica CCN-STIC-301 y la Guía CCN-STIC-430.

6.6. SECCIÓN 6. SERVICIOS PROPORCIONADOS POR EL SISTEMA

28. Deberán recogerse de forma resumida, todos los servicios proporcionados por el Sistema: servicio de almacenamiento de ficheros, servicio de correo electrónico, servicio de impresión, servicio de Back-Up, servicio Web, etc.

29. Deberá indicarse, para cada servicio, la norma de uso del mismo, los permisos y derechos establecidos y una breve descripción de su funcionamiento.

6.7. SECCIÓN 7. PROTOCOLOS Y PUERTOS HABILITADOS

30. Esta sección deberá proporcionar datos sobre los protocolos habilitados, la aplicación asociada a cada protocolo y el puerto asignado.

6.8. SECCIÓN 8. SEGURIDAD DE LAS TIC

31. Esta sección deberá proporcionar de forma resumida, datos relativos a los siguientes aspectos relacionados con la seguridad de las TIC:

    – La configuración del sistema operativo, pudiendo emplearse la correspondiente Guía STIC de configuración.
    – Las medidas establecidas para el control de acceso, la identificación y autenticación, el registro y la auditoría, la protección de la integridad y de la disponibilidad, la gestión de configuración y el nivel de garantía de los mecanismos empleados. Deberán indicarse, al menos, los requisitos recogidos en la Instrucción Técnica CCN-STIC-301 que sean de aplicación.
    – Las herramientas de seguridad instaladas.
    – El procedimiento establecido para el control, registro y protección de los dispositivos de almacenamiento removibles.
    – La seguridad criptológica:
        • Productos de cifra local (SW de cifrado de dispositivos removibles de almacenamiento, de cifrado de ficheros, etc.).
        • Material de cifra, empleado para la protección de las comunicaciones.
    – La seguridad de las emisiones: zoning de áreas, certificación de los equipos y/o las áreas, etc.

6.9. SECCIÓN 9. GESTIÓN DE LA SEGURIDAD DE LAS TIC

32. Esta sección deberá proporcionar de forma resumida, datos relativos a los siguientes aspectos relacionados con la gestión de seguridad del Sistema:

    – Procedimiento de gestión de incidentes (Guía CCN-STIC-403).
    – Plan de emergencia/contingencia del Sistema.
    – Informes a remitir durante el período de acreditación del Sistema.

6.10. SECCIÓN 10. SEGURIDAD FÍSICA

33. Los Sistemas deberán ubicarse en Zonas de Acceso Restringido acreditadas para el manejo de información clasificada.

34. Las Zonas de Acceso Restringido son instalaciones donde información clasificada CONFIDENCIAL o superior es almacenada o manejada por lo que deberán contar con las medidas y procedimientos de seguridad adecuados y suficientes, para asegurar la protección de la Información Clasificada en todo momento. Deberán estar organizadas conforme a alguna de las siguientes configuraciones de trabajo:

- AREA CLASE I: área en la que se maneja y almacena información clasificada de tal forma que la entrada a la zona supone, a todos los efectos, el acceso a la información clasificada, por lo que sólo puede acceder personal debidamente habilitado y autorizado. Se ubicarán en Áreas Clase I, servidores y cifradores.

- ÁREA CLASE II: área en la que se maneja y almacena información clasificada de tal forma que pueda estar protegida del acceso de personas no autorizadas mediante controles establecidos internamente, por lo que se podrá admitir la entrada a personal visitante debidamente controlado. Se ubicarán en Áreas Clase II, terminales y estaciones de trabajo.

35. Toda instalación en la que se vaya a almacenar o manejar material o información clasificados deberá someterse a un proceso de acreditación por el que se declara su constitución como Zona de Acceso Restringido.

36. La Acreditación es la autorización expresa que se otorga a una instalación, configurada como Área Clase I ó Área Clase II, especificando el origen y grado máximo de clasificación de la información que puede ser almacenada o manejada en la misma.

37. La competencia de Acreditación recae en la Oficina Nacional de Seguridad (ONS) como órgano de trabajo de la Autoridad Nacional de Seguridad (ANS), en el ámbito de su responsabilidad.

38. El proceso de Acreditación exigirá la elaboración, por parte del Responsable de Seguridad de la Zona de Acceso Restringido de un Plan de Protección. Dicho plan se deberá redactar conforme al modelo elaborado por la Oficina Nacional de Seguridad (ONS), cuyo modelo se adjunta como Anexo a este documento, el cual consta de tres documentos básicos:

    - **Plan de Acondicionamiento**: Su objeto es describir los sucesivos entornos de seguridad existentes, las características físicas y las medidas técnicas adoptadas, que permiten alcanzar un nivel de protección suficiente. No debe incluir, en ningún caso, procedimientos, normas o medidas organizativas, que sean objeto de los otros planes.
    - **Plan de Seguridad**: Su objeto es describir las medidas organizativas de seguridad, es decir, los procedimientos de control, gestión, trabajo, guarda, salvaguarda, etcétera, establecidos en el Órgano, Local o Área de Seguridad para, en conjunción con las medidas de seguridad física existentes (explicadas en el Plan de Acondicionamiento), permitir y garantizar la protección de la información clasificada y su adecuado manejo, en condiciones de trabajo habituales.
    - **Plan de Emergencia**: Su objeto es describir las medidas organizativas de seguridad a adoptar o seguir para mantener la protección de la información clasificada ante contingencias de tipo extraordinario que puedan afectar a la misma.

39. Los correspondientes Certificados de Acreditación se anexarán al documento abreviado.

6.11. SECCIÓN 11. SEGURIDAD EN EL PERSONAL

40. Esta sección deberá proporcionar datos relativos a las medidas de seguridad ligadas al personal, haciendo hincapié en los siguientes puntos, de no haber sido desarrollados en el **Plan de Seguridad**:

    – Requisitos para el acceso al Sistema (autorización y necesidad de conocer):
        - Usuarios.
        - Administradores.
    – Concienciación y formación del personal.

6.12. SECCIÓN 12. SEGURIDAD DOCUMENTAL

41. Esta sección deberá proporcionar datos relativos a las medidas de seguridad documental, haciendo hincapié en los siguientes puntos, de no haber sido desarrollados en el **Plan de Seguridad**:

    – Control y registro de los documentos y los soportes.
    – Control de las impresiones y las copias de documentos.
    – Normas de etiquetado de los documentos y de los soportes.
    – Proceso de destrucción de documentos y soportes.
    – Transferencia de documentos y soportes.

6.13. ANEXOS

42. Los anexos deben recoger toda aquella información que se considere de interés, pero que por su contenido no es recomendable incluirla en el cuerpo del documento abreviado. Deberían considerarse al menos, los siguientes anexos:

    – Formulario para la solicitud de alta en el Sistema.
    – Formulario para la notificación de incidentes.
    – Confirmación de haber leído y comprendido los POS.
    – Lista de personal autorizado con acceso a las áreas de seguridad.
    – Lista de personal autorizado con cuenta de usuario en el Sistema.
    – Lista de Criptocustodios.
    – Lista de Administradores.
    – Plan de Protección

ANEXO A. MODELO DE DOCUMENTO ABREVIADO

1. SOLICITUD Y ORGANIZACIÓN DE SEGURIDAD

DATOS DE LA SOLICITUD	
FECHA DE LA SOLICITUD:	
NOMBRE DEL ORGANISMO:	
DIRECCIÓN:	
UBICACIÓN:	
DENOMINACIÓN:	
ÁMBITO DE CLASIFICACIÓN:	
GRADO DE CLASIFICACIÓN DE LA INFORMACIÓN:	
MODO SEGURO DE OPERACIÓN:	
PERSONA DE CONTACTO (POC): (NOMBRE/EMPLEO/OFICINA/TELÉFONO/FAX/E-MAIL)	
ORGANIZACIÓN DE SEGURIDAD	
AOSTIC: (NOMBRE/EMPLEO/OFICINA/TELÉFONO/FAX/E-MAIL)	
RESPONSABLE DE SEGURIDAD DEL SISTEMA: (NOMBRE/EMPLEO/OFICINA/TELÉFONO/FAX/E-MAIL)	
ADMINISTRADOR DE SEGURIDAD: (NOMBRE/EMPLEO/OFICINA/TELÉFONO/FAX/E-MAIL)	
RESPONSABLE DE SEGURIDAD DEL ÁREA: (NOMBRE/EMPLEO/OFICINA/TELÉFONO/FAX/E-MAIL)	
RESPONSABLE DELEGADO DE SEGURIDAD: (NOMBRE/EMPLEO/OFICINA/TELÉFONO/FAX/E-MAIL)	
ADMINISTRADOR DEL SISTEMA: (NOMBRE/EMPLEO/OFICINA/TELÉFONO/FAX/E-MAIL)	

2. CONCEPTO DE OPERACIÓN

MISIÓN DEL SISTEMA

COMPOSICIÓN DEL SISTEMA	
Servidor	
Estaciones de trabajo	Nº
Router	
Cifrador	
impresoras	Nº

GRADO DE CLASIFICACIÓN Y MODO SEGURO DE OPERACIÓN
En la red se manejará información **Nacional/OTAN/UE/ESA...** clasificada hasta el grado de clasificación **.....**, en el modo seguro de operación**.....**. Sólo los usuarios con la AUTORIZACIÓN correspondiente y necesidad de conocer tendrán acceso al sistema**.**

AMENAZAS
Las principales amenazas a considerar son las que tienen por origen usuarios autorizados, la entrada de virus a través de soportes extraíbles o de correo remitido por otro nodo, y la realización de copias no controladas.

DOCUMENTACION DE REFERENCIA

3. DIAGRAMA DE LA RED CON DIRECCIONAMIENTO

4. CONFIGURACIÓN HARDWARE DEL SISTEMA

CARACTERÍSTICAS HARDWARE DEL SERVIDOR	
Marca/Modelo:	
Microprocesador:	
Memoria RAM:	
Disco Duro:	
Periféricos:	Disquetera 3½ / Unidad ZIP Lector/Grabador CD/DVD
Monitor:	
Teclado / ratón:	
Otra información:	

CARACTERÍSTICAS HARDWARE DE LAS ESTACIONES DE TRABAJO	
Marca/Modelo:	
Microprocesador:	
Memoria RAM:	
Disco Duro:	
Periféricos:	Disquetera 3½ / Unidad ZIP Lector/Grabador CD/DVD
Monitor:	
Teclado / ratón:	
Otra información:	

DISPOSITIVOS DE COMUNICACIONES Y PERIFÉRICOS DE LA RED	
Router (Marca/Modelo):	
Cifrador:	
Impresoras del Sistema:	
Escáner:	

5. CONFIGURACIÓN SOFTWARE DEL SISTEMA

CONFIGURACIÓN SOFTWARE DEL SERVIDOR	
Sistema Operativo (incluyendo versión):	
Servicios:	
Antivirus:	
Borrado seguro:	
SW de Seguridad:	

CONFIGURACIÓN SOFTWARE DE LAS ESTACIONES DE TRABAJO	
Sistema Operativo (incluyendo versión):	
Servicios:	
Antivirus:	
Borrado seguro:	
SW de Seguridad:	

6. SERVICIOS PROPORCIONADOS POR EL SISTEMA

SERVICIO DE ALMACENAMIENTO DE FICHEROS
POLÍTICA DE USO Todos los usuarios disponen de un recurso en el servidor de ficheros donde almacenar la información relativa a su actividad. Existen recursos asignados a grupos de usuarios relacionados con el área de actividad. El administrador del Sistema tiene la relación de los recursos activos en el Sistema. **PERMISOS Y DERECHOS** Ver Control de Accesos

SERVICIO DE CORREO ELECTRÓNICO

POLÍTICA DE USO

Todos los usuarios disponen de un cliente de correo electrónico para su uso dentro del Sistema. La política de uso de este servicio es:

- El servicio de correo electrónico tiene mecanismos de confidencialidad.
- Existen mecanismos de integridad, firma digital y acuse de recibo.
- Existen mecanismos de monitorización del Correo.
- Existen herramientas de registro y auditoría.
- Existe un servicio centralizado de salvaguarda de información.

PERMISOS Y DERECHOS

Se permite el uso del correo electrónico entre los usuarios del nodo.

Se permite el uso de correo electrónico con otros nodos mediante……

La autorización de correo entrante/saliente será realizado por el Responsable de Seguridad

SERVICIO DE IMPRESIÓN

POLITÍCA DE USO

Todos los usuarios disponen de una impresora asignada para la impresión de documentos en papel.

Las salidas de impresora de información clasificada se realizan a través de una sola impresora de red. La política establecida es la siguiente:

- Las impresoras en red están instaladas según figura en el diagrama del Sistema.
- El horario autorizado de utilización de ese servicio es.....
- El establecimiento de estos horarios, su control y las medidas para asegurar la distribución adecuada de los trabajos de impresión corresponde al Responsable de Seguridad.
- Se realiza una asignación exacta de impresoras a cada usuario.
- Solo se puede realizar una impresión de documentos si el usuario está autorizado para ello.
- Existe un control y una auditoría de las impresiones de los documentos clasificados.

PERMISOS Y DERECHOS

Sólo los usuarios autorizados pueden utilizar este servicio.

SERVICIO DE BACK-UP

POLITÍCA DE USO

El servicio de Back-up se realiza en el servidor por los administradores del Sistema:

- Semanalmente se realiza un back-up incremental en el servidor. Existen las copias necesarias entre los Back-up completos realizados mensualmente.
- Mensualmente se realiza un back-up completo. Se verifica el éxito del mismo y se almacena en..... Las copias mensuales se retienen 12 meses.
- Anualmente se realizan 2 back-ups completos, se verifica el éxito de los mismos y se almacenan en el lugar principal y alternativo .....……. Se mantienen copias de al menos los tres últimos años (dependiendo de la clasificación de la información).

PERMISOS Y DERECHOS

Para el acceso a los soportes de Back-up es necesario:

- Back-up semanal. Administrador del sistema con conocimiento del (administrador de seguridad / responsable de seguridad).
- Back-up mensual. Presencia de administrador de seguridad y administrador del sistema con conocimiento del responsable de seguridad.
- Back-up anual. Autorización expresa de la AOSTIC. Presencia de administrador de seguridad y administrador del sistema.

SERVICIO WEB (intranet)

POLÍTICA DE USO

La política es la siguiente:

- La información que la AOSTIC considere de interés se dispone en formato Web para permitir su consulta por los usuarios.
- Los navegadores Web de las diferentes estaciones de trabajo tienen una configuración segura.
- Sólo se habilitan los protocolos necesarios para este servicio.
- Se implementa una protección contra la modificación no autorizada de las páginas Web.
- Si se permite la consulta de información clasificada, se requiere una identificación y autenticación de usuarios para el acceso a determinadas páginas Web.
- Esta autenticación sigue la misma política de seguridad que la empleada para el resto del sistema.

PERMISOS Y DERECHOS

Sólo el administrador designado por la AOSTIC puede introducir contenidos en este servicio.

SERVICIO DE BASES DE DATOS
POLÍTICA DE USO Para el acceso a la base de datos se establece la siguiente política de uso: • Hay un control de acceso a la aplicación, a nivel de registro, y a nivel de campo. • Se establecen perfiles de usuario basados en la necesidad de conocer. • Existe un registro de auditoría, y se revisa periódicamente. • Existe un servicio centralizado de salvaguarda y recuperación de datos. • Hay una protección contra modificación/copia no autorizada. **PERMISOS Y DERECHOS** Sólo el personal designado por la AOSTIC puede introducir/modificar datos. Los usuarios pueden consultar datos de acuerdo a su necesidad de conocer.

7. PROTOCOLOS Y PUERTOS HABILITADOS

PROTOCOLO (*)	APLICACIÓN ASOCIADA/Observaciones	PUERTO
FTP	Uso de administración	20-21
telnet	Uso de administración	23
SMTP	Correo	25
POP 3	Correo	110
IMAP	Correo	143
DNS	Uso de administración	53
HTTP	Servicio Web (intranet)	80
SSH	Administración	22
SNMP	Gestión	161-162
SQL NET	Base de datos ORACLE	66

8. SEGURIDAD DE LAS TIC

CONFIGURACIÓN SISTEMA OPERATIVO

El Sistema Operativo está certificado (C2 según TCSEC / E2 según ITSEC / EAL3 según CC), y está configurado de acuerdo a la certificación.

Existe el siguiente mensaje de advertencia al acceder al Sistema:

"*Está usted accediendo a un Sistema que procesa información (Nacional/OTAN/UE/ESA)..... con grado de clasificación ..... Todo aquel usuario que tenga derecho a acceder a este Sistema está sujeto a todos los requerimientos especificados por la normativa de seguridad establecida. No está permitido el uso de disquetes, CD-ROM, o similares, sin la correspondiente autorización. El acceso no autorizado podrá dar lugar a las correspondientes acciones legales. El acceso al Sistema implica la aceptación expresa de las condiciones anteriores.*"

El desbloqueo de las estaciones de trabajo será realizado mediante contraseña.

La estación de trabajo se bloqueará a los 5 minutos de inactividad.

Sólo están activos los servicios, protocolos y puertos estrictamente necesarios para el desempeño de la función del Sistema.

CONTROL DE ACCESO

Los usuarios son identificados unívocamente en el Sistema mediante un nombre de usuario.

El administrador del Sistema establece los derechos de acceso a la información ..... clasificada.

Los accesos a los ficheros clasificados son registrados y auditados.

Los usuarios tienen acceso a los ficheros según su necesidad de conocer.

El administrador del Sistema tiene una relación en la que figuran los derechos de los usuarios en el Sistema.

Solamente los administradores del Sistema tienen acceso a la información de seguridad del Sistema.

Las directrices implantadas para el control de acceso del S.O. (Windows) son:

Se ha establecido el dominio …..... para todos los usuarios.

En este dominio se establecen cuentas de usuario donde se especifica:

- Nombre de usuario/contraseña.
- Grupos a los que pertenece.
- Derechos y permisos en el Sistema.
- Recursos accesibles.

En este dominio se establecen los siguientes grupos:

- Grupo de administradores con diferentes perfiles.
- Grupo de usuarios.

El control de acceso de los usuarios se establece según su necesidad de conocer.

AUTENTICACIÓN	
Los usuarios deben autenticarse antes de realizar cualquier acción en el Sistema.	Sí.
Las cuentas con privilegios de administración y de administración de seguridad son diferentes.	Sí.
Longitud mínima de las contraseñas	12 caracteres alfanuméricos
Validez máx./mín. de las contraseñas de las cuentas de usuario	90 días / 1 día
Validez máx./mín. de las contraseñas de las cuentas con privilegios.	60 días / 1 día
Máx. nº de intentos de acceso fallidos para bloqueo de la cuenta	3 intentos
No se pueden reutilizar las contraseñas en al menos	5 contraseñas
Generación de las contraseñas según un esquema predefinido.	Sí
Custodia de las contraseñas de cuentas con privilegios en sobres lacrados dentro de cajas fuertes.	Sí
Desbloqueo de las cuentas de usuario por el administrador.	Sí
Procedimiento de notificación de incidencias	Comunicación personal al administrador, e informe semanal de incidencias a la AOSTIC, o a quién ésta determine.

REGISTRO y AUDITORÍA

El sistema registra los siguientes eventos de seguridad:

- Encendido y apagado del Sistema.
- Inicio y cierre de sesión.
- Intentos de inicio de sesión
- Cambios en los permisos y privilegios de usuarios y grupos.
- Cambios en la información relevante de gestión de la seguridad del Sistema (incluyendo las funciones de auditoría).
- Arranque y parada de las funciones (servicios) de auditoría.
- Accesos a la información de seguridad del Sistema.
- Borrado, creación o modificación de los registros de auditoría.
- Cambios en la fecha y hora del Sistema.
- Intentos fallidos de acceder a los recursos del Sistema.
- Accesos a ficheros clasificados Confidencial/Reservado.
- Impresión de ficheros clasificados Confidencial/Reservado.

Por cada evento de seguridad se almacena la siguiente información:

- Número secuencial
- Tipo de Evento
- Éxito y fallo
- Fecha y hora
- Identidad del usuario que lo produce.

El registro de eventos es revisado semanalmente por la AOSTIC o por quién ésta determine.

La información de auditoría se guarda en lugar seguro por un período mínimo de dos (2) años.

Una vez revisados, los registros de eventos se almacenan en soporte cifrado con clave sólo utilizada por la AOSTIC o por quién ésta determine.

DISPOSITIVOS DE ALMACENAMIENTO REMOVIBLES

Existe un procedimiento de cifrado de los discos duros y soportes extraíbles clasificados.

La longitud mínima de la clave empleada para cifrar es de: 128 bits

Existe un procedimiento de borrado seguro de la información.

Los dispositivos se encuentran adecuadamente etiquetados y controlados según la información almacenada, y tienen la consideración de documento, por lo que es de aplicación lo establecido en el punto relativo a Seguridad Documental (apartado 1.9 de este procedimiento).

INTEGRIDAD

La configuración del sistema operativo se revisa cada 3 meses para verificar su integridad.

La configuración HW/SW se revisa cada 6 meses.

Cualquier modificación HW/SW se comunica a la AOSTIC mediante el formulario correspondiente.

Existe y está activo un SW de detección de código dañino, que revisa el Sistema al arrancar el mismo, y cada vez que se introduce un dispositivo removible. Se llevan a cabo actualizaciones al menos 1 vez a la semana.

DISPONIBILIDAD

Existe un procedimiento de copias de seguridad de la información:

Frecuencia	SEMANAL / MENSUAL / ANUAL
Lugar almacenamiento	(La información clasificada se almacenará conforme a su grado de clasificación y normativa que le afecte)
Lugar alternativo	

En caso de fallo será posible la restauración del Sistema. (Especificar el mismo)

Existe un control para el acceso autorizado a las copias de respaldo (Especificar el mismo)

GESTIÓN DE CONFIGURACIÓN

El diagrama del Sistema y de la red del apartado 1.2 se actualiza mensualmente.

Sólo se implementan las configuraciones HW/SW descritas en los correspondientes apartados.

En su caso se detallan las excepciones.

Se verifica al menos cada mes las configuraciones HW/SW del Sistema.

Solamente los administradores del sistema pueden llevar a cabo las configuraciones del sistema operativo de los ordenadores y de los servidores.

El equipamiento HW estará debidamente etiquetado y relacionado en inventario.

HERRAMIENTAS DE SEGURIDAD		
El control de la configuración de las herramientas de seguridad instaladas permanentemente, se lleva a cabo mediante los procedimientos de control de la configuración aplicables al resto de SW. No existen instalaciones temporales.		
Las herramientas de seguridad son controladas, y solamente las puede usar el personal específicamente autorizado para ello. Las herramientas implementan las actividades descritas en la Guía CCN-STIC-430, según la categoría de la herramienta. Se protege la información recopilada por las herramientas de seguridad. Las herramientas se actualizan de acuerdo a las recomendaciones del fabricante.		
SOFTWARE		**CERTIFICACIÓN**
Análisis de vulnerabilidades		
Detección de Intrusiones	DI versión 1.0.	EAL 3
Detección SW Dañino	DSWD versión 1.0.	EAL 2
Análisis de reg. de eventos	Se emplea la utilidad proporcionada por el Sistema Operativo.	EAL 4+ (Certificación del S.O.)
Monitorización de tráfico	MT versión 1.0	EAL 1
Mejora de la seguridad	No se han considerado necesarias por el resultado del análisis de riesgos.	
Cifrado SW	CSW versión 1.0	RESERVADO

8.1. SEGURIDAD CRIPTOLÓGICA

PRODUCTO DE CIFRA LOCAL
Se utiliza un producto certificado para cifrado de los dispositivos extraíbles y discos duros. Donde existen las siguientes claves: • Clave de disco duro para las estaciones de trabajo del Sistema. • Clave de intercambio para disquete. • Clave de intercambio para CD-ROM. • Clave del administrador de seguridad para auditorías. Las claves se generan por dispositivo certificado o proporcionadas por la correspondiente Autoridad. No se pueden utilizar soportes de almacenamiento sin cifrar dentro del CCI. La AOSTIC mantiene en sobre cerrado y lacrado las claves de los dispositivos cifrados, y se almacenan en lugar acorde a su clasificación. Las claves de intercambio se modifican cada año, registrándose la fecha del cambio y firma del responsable de dicha operación. No se almacena información en dispositivos que utilicen claves de intercambio.

MATERIAL DE CIFRA
Las claves se generan con dispositivo certificado o proporcionadas por la Autoridad correspondiente. El equipo de cifra está certificado para transmitir información clasificada hasta nivel CONFIDENCIAL/RESERVADO/SECRETO. El Oficial Criptocustodio es el responsable de la gestión de claves. El material de cifra se encuentra en un área de seguridad certificada. El material de cifra se encuentra protegido por las etiquetas de seguridad aprobadas.

8.2. SEGURIDAD DE LAS EMISIONES

SEGURIDAD EMISIONES	
La red se encuentra en un local certificado como ZONA 3.	
Los equipos se han instalado de acuerdo a la normativa TEMPEST y a la certificación del local.	

9. GESTIÓN DE SEGURIDAD DE LAS TIC

GESTIÓN DE INCIDENTES

Existe un formulario para la comunicación de incidentes de seguridad, recogido en un anexo a este documento.

Los incidentes de seguridad deberán ser comunicados a la AOSTIC y a la Autoridad responsable de la acreditación siguiendo el procedimiento establecido.

Se informa de los incidentes de seguridad en el INFORME ANUAL a remitir.

PLAN DE EMERGENCIA/CONTINGENCIA

El responsable de realizar las copias de seguridad es .....

El lugar de almacenamiento de las copias de seguridad es acorde a su clasificación.

En caso de emergencia, existe un procedimiento de destrucción de la información contenida en soportes extraíbles.

Cualquier fallo HW/SW se comunica a la AOSTIC.

Se prueban trimestralmente las copias de seguridad por .....

La notificación de incidentes se realiza a la AOSTIC mediante formulario del anexo 3.

INFORMES DURANTE EL PERÍODO DE ACREDITACIÓN

Durante el mes de Enero de cada año se remitirá un informe a la Autoridad responsable de la acreditación con:

- Las altas y bajas de personal usuario, técnico y de administración del Sistema.
- Las modificaciones previstas para el año siguiente.
- El estado de cumplimiento de las modificaciones previstas en el informe del año anterior.
- Los incidentes de seguridad ocurridos en ese año.

Cualquier otro cambio que sufra el Sistema, de emplazamiento o de configuración hardware/software, no previsto en el informe remitido será comunicado por la AOSTIC a la Autoridad responsable correspondiente para reiniciar el proceso de acreditación del Sistema.

10. SEGURIDAD FÍSICA

ENTORNO GLOBAL DE SEGURIDAD (EGS)

Las medidas de seguridad del edificio donde se ubican los elementos del Sistema deben citarse en el Plan de Protección (constituido por los Planes de Acondicionamiento, Seguridad y Emergencia, conforme al modelo incluido en el Anexo B de este documento). Este apartado incluirá, por tanto, la referencia de dicho documento.

ENTORNO LOCAL DE SEGURIDAD (ELS)

Las áreas de seguridad donde se ubica la red están certificadas para el manejo de información (Nacional/OTAN/UE/ESA)..... clasificada hasta el grado de clasificación ..... Sus certificados se anexan a este documento.

Estas áreas de seguridad están documentadas mediante los correspondientes planes de Acondicionamiento, de Seguridad, y de Emergencia, conforme al modelo existente, y que formarán parte como Anexo al CO/DRES/POS. Este apartado incluirá, por tanto, la referencia de dicho documento.

El personal de apoyo (limpieza, mantenimiento, etc.) accede a las áreas de seguridad acompañado por usuarios autorizados.

Existe un registro de accesos que se comprueba semanalmente.

La AOSTIC es responsable de los accesos a las áreas de seguridad.

El acceso de visitas a las áreas de seguridad debe ser autorizado por ..... (la AOSTIC o por quién ésta haya determinado).

No se permite la introducción de dispositivos informáticos portátiles, ni de dispositivos de comunicación portátiles en las áreas de seguridad del Sistema.

Se han establecido procedimientos adecuados para evitar la visualización y el acceso a la información manejada en las áreas de seguridad, cuando accedan visitas a las mismas.

ENTORNO DE SEGURIDAD ELECTRÓNICO (ESE)

La autenticación de usuarios está basada en (nombre de usuario y contraseña/mecanismos criptográficos/mecanismos biométricos).

Cifrado de la información.

Sistemas contra la manipulación de los equipos (etiquetas de seguridad).

11. SEGURIDAD EN EL PERSONAL

SEGURIDAD DEL PERSONAL
Las medidas específicas de seguridad del personal deben citarse en el Plan de Protección (constituido por los Planes de Acondicionamiento, Seguridad y Emergencia, conforme al modelo incluido en el Anexo B de este documento). Este apartado incluirá, por tanto, la referencia de dicho documento. Todo el personal que accede a las áreas de seguridad donde se ubican los equipos del Sistema dispone de la autorización correspondiente. Se identifica y autentica todo el personal que accede a las áreas de seguridad. El personal de administración dispone de autorización específica de la AOSTIC. El personal con acceso autorizado tiene la debida necesidad de conocer. El personal está concienciado, y ha recibido la adecuada formación e instrucción en materia de seguridad.

12. SEGURIDAD DOCUMENTAL

SEGURIDAD DOCUMENTAL
En el Plan de Protección (constituido por los Planes de Acondicionamiento, Seguridad y Emergencia, conforme al modelo incluido en el Anexo B de este documento) se habrán citado ya los procedimientos generales de control y manejo de documentos. Este apartado incluirá, por tanto, la referencia de dicho Plan, y se añadirán aquellas medidas no incluidas en el mismo, que normalmente derivarán de la existencia de un sistema CIS en el área de seguridad. El Órgano de Control del que depende, a efectos de manejo y gestión de la información clasificada, es: ..... La documentación, con independencia del soporte, se maneja y controla conforme a la normativa de seguridad que le afecta. Se registran y contabilizan todos los accesos a los documentos clasificados. Todos los documentos y soportes clasificados se etiquetan de acuerdo al procedimiento establecido. Se controlan todas las entradas/salidas de soportes de información.

Todos los dispositivos de almacenamiento de información clasificada están registrados por el Órgano de Control correspondiente.

Los soportes se almacenan en un lugar acorde a su clasificación.

La producción de copias (reproducción) se realiza según el procedimiento fijado.

La destrucción de información se realiza según procedimiento aprobado (indicar procedimiento y normativa en que se basa).

Todos los soportes de almacenamiento que entren/salgan del Entorno de Seguridad Electrónica (ESE) se cifran mediante producto certificado, o se implementarán las medidas de seguridad físicas adecuadas.

Se controlan todas las impresiones de los documentos.

La transferencia de información usando soportes de almacenamiento removibles se realiza de la siguiente forma:

- El punto de entrada/salida es el ordenador utilizado y etiquetado como aduana.
- La AOSTIC, o quien éste determine, descifra los soportes cifrados, y verifica y registra la información de entrada/salida.
- No existen soportes de almacenamiento sin cifrar dentro del Circuito Cerrado de Información (CCI) que forma el Sistema. La salida/entrada de soportes de cifrados que contienen información clasificada Confidencial/Reservado debe ser autorizada por la AOSTIC, o quién ésta determine.
- La salida de información clasificada Confidencial/Reservado sin cifrar requiere la autorización de la AOSTIC.
- Semanalmente se audita el registro de entrada/salida de soportes.
- Se ejecutan los procedimientos antivirus aprobados.

……., …… DE……..DE ……

LA AUTORIDAD OPERATIVA DEL SISTEMA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

ANEXOS

FORMULARIO PARA LA SOLICITUD DE ALTA EN EL SISTEMA

Solicitud de alta en el sistema	De:			Sistema			Fecha
Acción	Nombre del usuario	Empleo	Órgano	Oficina	Teléfono	Nivel de Autorización	Tipo de usuario
Comentarios (justificación):							
AOSTIC			Firma				Fecha
Responsable de la seguridad del Sistema			Firma				Fecha
Administrador del Sistema			Firma		Fecha de recepción		Fecha de alta

FORMULARIO PARA LA NOTIFICACIÓN DE INCIDENTES

1. INFORMACIÓN GENERAL DE CONTACTO	
1.1. Nombre:	1.2. Despacho:
1.3. Teléfono:	1.4. Organismo:
1.5. Información adicional de contacto:	1.6. Fecha de comunicación del incidente:
2. INFORMACION DEL EQUIPO	
2.1. Naturaleza del equipo (PC, cifrador, router, servidor, etc.)	2.2. Codificación del equipo
2.3. Configuración hardware:	
2.4. Configuración software:	
2.5. En caso de tratarse de una estación de trabajo.	
2.5.1. Sistema Operativo, versión y service-pack instalado:	
2.5.2. ¿Está integrado en una red?	
2.5.3. ¿Configuración del dominio?	
2.5.4. Nombre de usuario en el dominio:	
2.5.5. Grupos a los que pertenece:	
2.5.6. Derechos asociados:	
2.5.7. Funciones encomendadas.	
2.5.8. Dirección IP	

3. INFORMACIÓN DEL INCIDENTE			
3.1 Hora de notificación del incidente	3.2 Fecha y duración del incidente		
3.3 ¿Cómo se descubrió el incidente?			
3.4 Naturaleza de la información manejada en la máquina involucrada			
3.5 Importancia del incidente: Leve - Medio - Grave	3.6 Clasificación de la información involucrada: Desconocido - Sin Clasificar - Confidencial - Reservado - Secreto		
3.7 Grado de compromiso de la información: Improbable - Probable - Seguro			
3.8 La incidencia impide el correcto flujo documental interno de la Organización:		SI	NO
3.9 La incidencia impide el correcto flujo documental externo de la Organización:		SI	NO
3.10 Descripción del incidente:			

3.11 Categoría del incidente de seguridad:			
Intento de acceso no autorizado al sistema.		Interrupción no prevista del funcionamiento o denegación de servicio.	
Interceptación, modificación, introducción, corrupción, destrucción o divulgación de información no autorizada.		Abuso de privilegios de acceso.	
Cambios no autorizados en las características y configuración del software, conocidos o consentidos por el usuario.		Cambios no autorizados en las características y configuración del hardware, conocidos o consentidos por el usuario.	
Prueba, sondeo, broma o suplantación de identidad.		Utilización no autorizada de un equipo/ máquina / sistema.	
Ataque procedente de la red.		Suplantación de dirección IP.	
Vulnerabilidad del producto.		Errores de configuración.	
Mal uso de los recursos de la máquina.		Software malicioso (virus, etc.).	
Irregularidades en el correo electrónico.		Emanaciones electromagnéticas.	
Divulgación de datos sensibles del sistema por ingeniería social		Errores de mantenimiento.	
Otros			

3.12 Origen / Fuente / Causa del incidente:
3.13 Valoración personal sobre la intencionalidad del incidente:
3.14 Medidas tomadas después del incidente:
3.15 Estado de resolución del incidente:

DECLARACIÓN DE HABER LEÍDO LOS POS

Certifico haber leído y comprendido los Procedimientos Operativos de Seguridad del Sistema .....:

Usuario: _____

Nombre y empleo: _____

Despacho y extensión: _____

Fecha: _____

Firma: _____

Fecha de activación de la cuenta de usuario _____

Responsable de seguridad: _____

Despacho y extensión: _____

Firma: _____

LISTA DE PERSONAL AUTORIZADO CON ACCESO A LAS ZONAS DE ACCESO RESTRINGIDO

PERSONAL CON ACCESO A LA PLANTA

- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....

PERSONAL CON ACCESO A LA SALA DE SERVIDORES

- .....
- .....
- .....
- .....

PERSONAL CON ACCESO A LA SALA DE MATERIAL DE CIFRA

- .....
- .....

LISTA DE PERSONAL AUTORIZADO CON CUENTA DE USUARIO EN EL SISTEMA

- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....

LISTA DE CRIPTOCUSTODIOS

CRIPTOCUSTODIO

– .....

CRIPTOCUSTODIO ALTERNATIVO

– .....

LISTA DE ADMINISTRADORES

ADMINISTRADORES DEL SISTEMA

- .....
- .....

ADMINISTRADORES DE SEGURIDAD SISTEMA

- .....

ANEXO B. PLAN DE PROTECCIÓN

1. PLAN DE ACONDICIONAMIENTO

1.1. OBJETO

(Definir la finalidad del plan, y la identificación/definición exacta del Órgano, Local o Área de Seguridad al que se refiere)

1.2. SITUACIÓN

(Explicar la localización física del Órgano, Local o Área de Seguridad dentro del Edificio, Acuartelamiento, Base, Centro, etcétera, en que se encuentre. Si es preciso y relevante, se indicará la situación en el entorno exterior – ciudad, terreno colindante -)

1.3. PLANOS

(Referencia de los planos, que se incorporarán como anexos al plan; se incluirán los generales de entorno, Base, Zona, Edificio y Planta, con indicación de la situación en los mismos del Órgano, Local o Área de Seguridad, y se incluirán los planos de detalle de este último, en planta y alzado, con indicación detallada de los elementos relevantes para la seguridad, tanto del propio local, como de los elementos de seguridad adicionales instalados y del mobiliario de seguridad. En este sentido es importante reflejar la situación de sensores, lectores, cámaras CCTV, cajas y armarios de seguridad, destructora de papel, fotocopiadora, mobiliario habitual, disparadores de extinción, etcétera)

1.4. DESCRIPCIÓN

1.4.1. ELEMENTOS ESTRUCTURALES

1.4.1.1. PARAMENTOS HORIZONTALES Y VERTICALES

(Descripción de muros, suelo, techo, falsos techos y existencia o no de ventanas o huecos en paramentos, del Local o Área, principalmente de los que constituyen el perímetro, con indicación de su constitución, grosor y fortaleza. Indicación de instalación de sistemas de insonorización)

1.4.1.2. PUERTAS

1.4.1.2.1. DESCRIPCIÓN

(Características físicas de las puertas y marcos, con indicación de su constitución y fortaleza. Se hará una descripción para cada puerta existente)

1.4.1.2.2. SISTEMA(S) DE APERTURA

(Descripción de los instalados en las puertas, con sus características de seguridad, modelo, fortaleza)

1.4.1.2.3. SISTEMA(S) DE SEGURIDAD

(Descripción de los instalados en las puertas, para impedir o detectar su apertura no autorizada, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

1.4.1.3. VENTANAS

1.4.1.3.1. DESCRIPCIÓN

(Características físicas de las ventanas y marcos, con indicación de su constitución y fortaleza. Altura respecto al suelo exterior más próximo y accesibilidad desde el exterior. Visibilidad desde el exterior y elementos para impedir dicha visibilidad. Se hará una descripción para cada ventana cuando sea preciso)

1.4.1.3.2. REJAS

(Características físicas, constitución, grosor, paso entre barras, distancias, anclajes a pared, situación)

1.4.1.3.3. SISTEMA(S) DE APERTURA

(Descripción de los instalados en las ventanas, con sus características de seguridad, modelo, fortaleza)

1.4.1.3.4. SISTEMA(S) DE SEGURIDAD

(Descripción de los instalados en las ventanas, para impedir o detectar su apertura no autorizada, o la rotura de cristales, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

1.4.1.4. HUECOS

1.4.1.4.1. DESCRIPCIÓN

(Características físicas de los huecos, con indicación de su tamaño, forma, situación, accesibilidad desde el exterior. Altura respecto al suelo exterior más próximo. Se hará una descripción para cada ventana cuando sea preciso)

1.4.1.4.2. REJAS

(Características físicas, constitución, grosor, paso entre barras, distancias, anclajes a pared, situación)

1.4.1.4.3. SISTEMA(S) DE SEGURIDAD

(Descripción de los instalados en cada hueco, para impedir o detectar su paso no autorizada, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

1.4.2. ELEMENTOS DE SEGURIDAD

1.4.2.1. SISTEMA(S) DE CONTROL DE ACCESOS

1.4.2.1.1. DESCRIPCIÓN

(Tipo, funcionamiento, características generales, mantenimiento)

1.4.2.1.2. SISTEMA(S) DE SEGURIDAD

(Elementos adicionales de seguridad implementados en el sistema de control de accesos: "antipass-back", alarma antisabotaje, sensor de presencia en esclusas, conexión a sistema alternativo de energía, interfonos, etcétera, e indicación del modo de transmisión de alarmas)

1.4.2.2. SISTEMA(S) DE DETECCIÓN DE INTRUSIÓN (IDS)

1.4.2.2.1. DESCRIPCIÓN

(Tipo, funcionamiento, características generales, mantenimiento)

1.4.2.2.2. SISTEMA(S) DE SEGURIDAD

(Elementos adicionales de seguridad implementados en el sistema IDS: detección antisabotaje, sistema de autochequeo automático, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

1.4.2.3. SISTEMA(S) DE CIRCUITO CERRADO DE TV (CCTV)

1.4.2.3.1. DESCRIPCIÓN

(Tipo, funcionamiento, características generales, mantenimiento)

1.4.2.3.2. SISTEMA(S) DE SEGURIDAD

(Elementos adicionales de seguridad implementados en el sistema CCTV: detección antisabotaje, sistema de autochequeo automático, interconexión con sistema IDS, conexión a sistema alternativo de energía, etcétera, e indicación del modo de transmisión de alarmas)

1.4.2.4. SISTEMA DE PROTECCIÓN TEMPEST

1.4.2.4.1. MEDIDAS TEMPEST

(Descripción de las medidas TEMPEST adoptadas en los locales y medios instalados

1.4.2.4.2. MEDICIÓN TEMPEST

(Si el Órgano, Local o Área de Seguridad ha sido objeto de un medición TEMPEST, indicarlo, con expresión de quien lo ha realizado y los resultados de medición obtenidos –clasificación-)

1.4.2.5. SISTEMAS DE DESTRUCCIÓN

1.4.2.5.1. DESTRUCTORAS DE PAPEL

(Tipo, modelo, características de corte, capacidad)

1.4.2.5.2. OTROS ELEMENTOS DE DESTRUCCIÓN

(Tipo, modelo, características, capacidad – incluir sistemas de emergencia previstos)

1. 4.2.6. MEDIOS DE REPRODUCCIÓN

(Tipo, modelo, almacenamiento en memoria, identificación de usuario. Se debe conocer si la máquina mantiene datos en memoria tras cada fotocopia realizada; debe configurarse para que no los mantenga, o establecer un procedimiento de borrado en el Plan de Seguridad).

1.4.2.7. SISTEMA CONTRA-INCENDIOS

(Tipo, características)

1.4.2.8. SISTEMA(S) ALTERNATIVO DE ENERGÍA

(Descripción general del sistema y de su utilidad a nivel de la seguridad)

1.4.3. MOBILIARIO DE SEGURIDAD

1.4.3.1. CAJAS FUERTES

1.4.3.1.1. DESCRIPCIÓN

(Características físicas, con indicación de su constitución, peso, fortaleza y protección contra el agua y el fuego. Se hará una descripción para cada caja existente)

1.4.3.1.2. SISTEMA(S) DE APERTURA

(Descripción de los instalados en las puertas, con sus características de seguridad, modelo, fortaleza, número de combinaciones posibles, llaves)

1.4.3.1.3. SISTEMA(S) DE SEGURIDAD

(Descripción de los instalados, para impedir o detectar su apertura o traslado no autorizados, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

1.4.3.2. ARMARIOS BLINDADOS

1.4.3.2.1. DESCRIPCIÓN

(Características físicas, con indicación de su constitución, fortaleza y protección contra el agua y el fuego. Se hará una descripción para cada armario blindado existente)

1.4.3.2.2. SISTEMA(S) DE APERTURA

(Descripción de los instalados en las puertas, con sus características de seguridad, modelo, fortaleza, número de combinaciones posibles, llaves)

1.4.3.2.3. SISTEMA(S) DE SEGURIDAD

(Descripción de los instalados, para impedir o detectar su apertura o traslado no autorizados, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

1.4.3.3. CONTENEDORES DE SEGURIDAD

1.4.3.3.1. DESCRIPCIÓN

(Características físicas, con indicación de su constitución, fortaleza y protección contra el agua y el fuego. Se hará una descripción para cada contenedor existente)

1.4.3.3.2. SISTEMA(S) DE APERTURA

(Descripción de los instalados en las puertas o archivadores, con sus características de seguridad, modelo, fortaleza, número de combinaciones posibles, llaves)

1.4.3.3.3. SISTEMA(S) DE SEGURIDAD

(Descripción de los instalados, para impedir o detectar su apertura o traslado no autorizados, como sensores, etcétera, e indicación del modo de transmisión de alarmas)

1.4.4. ELEMENTOS DE PROTECCIÓN EXTERIOR

1.4.4.1. DEL EDIFICIO

(Descripción resumida y general de los elementos físicos de seguridad relevantes del Edificio en que se encuentra el Órgano, Local o Área de Seguridad)

1.4.4.2. EXTERIOR AL EDIFICIO

(Descripción resumida y general de los elementos físicos de seguridad relevantes de posibles perímetros de seguridad exteriores al edificio)

1.4.5. OTROS ELEMENTOS DE SEGURIDAD RELEVANTES

(Es posible que existan otras medidas de seguridad instaladas, o llevadas a efecto, en el Órgano, Local o Área de Seguridad, como por ejemplo: sistemas de supresión de señales, “barridos” realizados para detección de elementos activos de escucha; de todos ellos se dará información en este apartado).

2. PLAN DE SEGURIDAD

2.1. OBJETO

(Definir la finalidad del Plan de Seguridad. Nivel de clasificación superior de la información que va a ser protegida y manejada, y tipo – OTAN, UE -)

2.2. ÁMBITO DE APLICACIÓN

(Alcance del plan. Identificación/definición exacta del Órgano, Local o Área de Seguridad y motivo por el que se constituye. Organismo, Departamento o Unidad al que se da servicio)

2.3. DEPENDENCIA

2.3.1. DEPENDENCIA DE MANDO

(Identificación del órgano superior, externo al Órgano, Local o Área de Seguridad, del que se depende a efectos orgánicos o de mando)

2.3.2. DEPENDENCIA FUNCIONAL

(Identificación del órgano externo del que se depende funcionalmente respecto a protección de la información clasificada, dentro de la cadena de la infraestructura de protección)

2.4. CONCEPTO GENERAL DE SEGURIDAD

2.4.1. ENTORNOS DE SEGURIDAD

2.4.1.1. ENTORNO GLOBAL

(Descripción general de las medidas de seguridad establecidas en el Acuartelamiento, Base, Edificio u Órgano superior dentro del que se encuentra. No se citarán, salvo que sea preciso para aclarar otros conceptos, los elementos ya explicados en el Plan de Acondicionamiento. Se atenderá principalmente a: Control general de accesos, existencia de guardias de seguridad, patrullas y fuerzas de reacción, sistemas generales para identificación de visitas, todo ello siempre en la parte en que pueda aportar medidas adicionales de seguridad a las propias del Órgano, Local o Área de Seguridad)

2.4.1.2. ENTORNO LOCAL

(Descripción general y somera de las medidas de seguridad establecidas en el propio Órgano, Local o Área de Seguridad. No se entrará en detalle, dado que en los siguientes apartados se tratarán en profundidad. Principalmente se citará que en este entorno rigen normas especiales de seguridad, que llevarán un tratamiento específico en el Plan de Protección, y se darán unas pinceladas de los mismos)

2.5. PERSONAL DEL ÓRGANO, LOCAL O ÁREA DE SEGURIDAD

(Descripción de los puestos de trabajo existentes dentro del Órgano, Local o Área de Seguridad, especialmente los que tengan responsabilidades superiores en seguridad –Jefe de Seguridad, Adjunto, Oficial de Control COSMIC o ATOMAL, etcétera -. No es precisa relación nominal, únicamente la descripción del puesto. En lugares con gran cantidad de personal, se indicará el número de personas por tipos de puestos o similares, destacando sólo los puestos relevantes. Sobre estas personas se llevará el control de acceso diario)

2.6. PROCEDIMIENTOS DE SEGURIDAD

2.6.1. CONTROL DE PERSONAL

2.6.1.1. GESTIÓN DE USUARIOS AUTORIZADOS

(Procedimiento para el control, altas y bajas, del personal destinado en el Órgano, Local o Área de Seguridad o personal autorizado. Mantenimiento de listados. Identificación visual del personal. Procedimiento de gestión de habilitaciones personales de seguridad –HPS-. Posibles restricciones de acceso a la información para determinados puestos.)

2.6.1.2. GESTIÓN DE PERSONAL DE LIMPIEZA Y MANTENIMIENTO

(Procedimiento para el control, altas y bajas. Mantenimiento de listados. Identificación visual del personal. Escolta. Necesidad de HPS.)

2.6.1.3. HORARIO DE TRABAJO

(Descripción del horario de trabajo, con indicación de tiempos con presencia o no de personal. Procedimiento para permanecer en zona fuera de horas de trabajo y restricciones al respecto. Personal presente las 24 horas. Servicios)

2.6.1.4. FORMACIÓN DEL PERSONAL

(Descripción del procedimiento para mantener la instrucción y concienciación del personal autorizado para acceso a la zona, en materia de seguridad en el manejo y protección de la documentación.)

2.6.2. CONTROL DE ACCESO AL ÓRGANO, LOCAL O ÁREA DE SEGURIDAD

2.6.2.1. GESTIÓN DE USUARIOS

(Descripción detallada de procedimientos para alta y baja de usuarios, permisos necesarios, control de usuarios, listados, asignación de números de identificación personal, elaboración de tarjetas de acceso, dentro del sistema de control de accesos disponible)

2.6.2.2. PROCEDIMIENTO DE ACCESO

(Descripción detallada del procedimiento a seguir por los usuarios autorizados, para acceder al Órgano, Local o Área de Seguridad, con indicación explícita de la forma de evitar la mala práctica de que personas autorizadas permitan el acceso a otras, no quedando registrado su acceso. Explicar cómo se realiza la identificación del usuario. Acceso fuera de horario de trabajo y control de dichos accesos)

2.6.2.3. GESTIÓN DE SEGURIDAD

(Descripción detallada del procedimiento de control y auditoría de accesos, responsabilidades en este aspecto, actuación ante pérdidas de tarjetas o revelación de número personal)

2.6.2.4. VISITAS

(Descripción detallada del procedimiento de control de acceso para la visitas. Indicar si están permitidas o no, o en qué circunstancias se permiten. Existencia de Libro de Registro de Visitas y procedimiento para cumplimentarlo. Procedimiento de identificación y escolta de visitas)

2.6.3. CONTROL DE LLAVES

(Descripción detallada del procedimiento para su manejo, control, sustitución, registro de cambios de cerraduras, actuación ante pérdidas, custodia durante y después del trabajo. Si existen diferencias, se indicará el procedimiento para cada llave que tenga un tratamiento diferente –normalmente no tendrá el mismo trato la llave de la puerta que la llave de la caja fuerte-)

2.6.4. CONTROL DE CLAVES DE COMBINACIÓN

(Descripción detallada del procedimiento para su manejo, control, sustitución, registro de cambios de claves y motivos, actuación ante pérdidas o comprometimientos, actuación por cambio de personal, custodia segura de claves para emergencias)

2.6.5. ACTIVACIÓN SISTEMA IDS Y SENSORES

(Descripción detallada del procedimiento y horario, o eventos necesarios, para su activación/desactivación. Verificación diaria de funcionamiento. Posibles tiempos muertos sin cobertura. Activación a final de jornada. Desactivación a principio de jornada. Otras activaciones/desactivaciones)

2.6.6. ACTUACIÓN ANTE ALARMAS

2.6.6.1. SISTEMA DE RECEPCIÓN DE ALARMAS

(Descripción detallada del procedimiento para la transmisión y recepción de alarmas. Verificación diaria de funcionamiento)

2.6.6.2. ACTUACIÓN ANTE ALARMAS

(Actuación del Centro de Recepción de Alarmas. Procedimiento para la comunicación y actuación del personal implicado en la respuesta – guardia, fuerzas de reacción, responsables de seguridad. Tiempos de respuesta. Ensayos de alarma)

2.6.7. GUARDIA DE SEGURIDAD

(Descripción detallada de los apoyos en seguridad prestados, por el personal de guardia o servicio de vigilancia, que afectan directamente a la seguridad del Órgano, Local o Área de Seguridad, en forma de rondas, inspecciones a fin de jornada, vigilancia exterior, etcétera)

2.6.8. CORTES DE ENERGÍA

(Descripción detallada del procedimiento de actuación ante un corte de energía, en función de los sistemas alternativos existentes. Normas de protección especiales a adoptar en caso de fallos que afecten a los sistemas: sensores, IDS, control de accesos)

2.6.9. CONTROL DE LA DOCUMENTACIÓN

2.6.9.1. CONTROL DOCUMENTAL

(Descripción detallada de la forma en que se realiza el registro de entrada y salida, y la distribución de documentos. Movimiento y traslado de documentación clasificada. Tratamiento de mensajes. Tratamiento de documentos clasificados recibidos por canales no habituales. Copias de seguridad de los registros y almacenamiento de las mismas en local diferente)

2.6.9.2. PROCEDIMIENTO DE ALMACENADO

(Descripción detallada de la forma en que se almacena la información clasificada en los contenedores, cajas fuertes o armarios blindados. Criterios de almacenamiento. Separación en contenedores diferentes de la información clasificada de diferentes tipos –OTAN, UE -. Separación por niveles de clasificación)

2.6.9.3. PROCEDIMIENTO DE ACCESO

(Descripción detallada del procedimiento de acceso a la documentación almacenada por parte del personal autorizado, distinguiendo entre el propio personal destinado en el Órgano, Local o Área de Seguridad, y el que, sin estarlo, tiene la necesidad de conocer, está habilitado y es autorizado para acceder a dicha información. Existencia de salas de lectura. Criterios para que un usuario pueda retirar información clasificada y condiciones –bajo responsabilidad del Jefe de Seguridad y cumpliendo la normativa vigente-)

2.6.9.4. PROCEDIMIENTO DE REPRODUCCIÓN

(Descripción detallada del procedimiento de fotocopiado de documentos clasificados. Personal autorizado. Registro de copias)

2.6.9.5. PROCEDIMIENTO DE DESTRUCCIÓN

(Descripción detallada del procedimiento para la destrucción ordinaria de la información clasificada. Responsabilidades. Testigos)

2.6.10. LISTA DE COMPROBACIÓN DIARIA

(Lista detallada de las tareas diarias de comprobación que de forma automática, aunque con atención, deben realizarse al inicio y final de jornada para verificar que las condiciones de seguridad están establecidas y no ha habido ninguna violación de las mismas)

2.6.11. INFORMES DE VIOLACIONES O COMPROMETIMIENTOS

(Procedimientos y canales de comunicación de posibles comprometimientos de la información clasificada o de violaciones de la seguridad)

2.6.12. OTROS PROCEDIMIENTOS DE SEGURIDAD RELEVANTES

(Se indicará cualesquiera otros que sean precisos para definir de forma exhaustiva la seguridad implantada, y que no tengan encaje en los puntos anteriores)

3. PLAN DE EMERGENCIA

3.1. OBJETO

(Definir la finalidad del Plan de Emergencia)

3.2. TIPOS DE EMERGENCIA

(Enumeración esquemática de los diferentes tipos de emergencia que se van a considerar en este plan. Se pueden clasificar por diferentes criterios, o combinaciones de varios:

– Tipo: incendio, inundación, acto terrorista, disturbios

– Continuidad: abandono del local, aumento de medidas de protección por imposibilidad de abandono.

– Consecuencias: material clasificado afectado, no afecta al material.)

3.3. PROCEDIMIENTOS GENERALES DE ACTUACIÓN

3.3.1. ACTUACIÓN AL PRODUCIRSE LA EMERGENCIA

3.3.1.1. EN HORARIO DE TRABAJO

(Procedimientos generales a seguir. Determinación del tipo de emergencia. Responsable de inicio de actuaciones. Guardado de la información. Cierre de contenedores. Evacuación del personal. Avisos. Teléfonos de emergencias)

3.3.1.2. FUERA DE HORARIO DE TRABAJO

(Procedimientos generales a seguir. Avisos necesarios. Actuación primera de los servicios de vigilancia. Responsabilidades. Criterios de acceso a la zona clasificada. Teléfonos de emergencias)

3.3.2. ACTUACIONES POSTERIORES

3.3.2.1. TRASLADO DE LA DOCUMENTACIÓN CLASIFICADA

(Criterios para adoptar la decisión del traslado. Responsabilidades. Prioridades. Procedimientos generales a seguir en caso de que se decida esta actuación. Instalaciones previstas. Itinerarios y planos de evacuación. Medios. Avisos. Recuentos. Actas del movimiento)

3.3.2.2. DESTRUCCIÓN DE LA DOCUMENTACIÓN CLASIFICADA

(Procedimientos generales a seguir en caso de que se decida esta actuación. Responsabilidades. Criterios. Prioridades. Medios. Avisos. Lugares alternativos previstos para la destrucción masiva)

3.3.2.3. EVALUACIÓN DE DAÑOS E INFORMES

(Procedimiento para el recuento de la información clasificada, análisis de pérdidas, certificados de destrucción, informes de comprometimientos y pérdidas)

3.3.2.4. VUELTA A LA SITUACIÓN INICIAL

(Procedimientos generales a seguir y requisitos a cumplir, una vez finalizada la situación de emergencia, para la vuelta a la situación inicial. Mecanismos de recuperación de la información. Condiciones de seguridad mínimos necesarios

3.4. PROCEDIMIENTOS PARTICULARES DE ACTUACIÓN

(Descripción, para cada tipo de emergencia considerado, de las actuaciones, complementarias o más detalladas, que las generales indicadas anteriormente, que sería preciso ejecutar para asegurar la protección de la información clasificada)

ANEXO C. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Acreditación	Autorización otorgada por la Autoridad responsable de la acreditación, para manejar información nacional clasificada hasta un grado determinado, o en unas determinadas condiciones de integridad o disponibilidad, con arreglo a su concepto de operación.
Amenaza	Eventos que pueden desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Análisis o valoración de Riesgos	Proceso sistemático para estimar la magnitud del riesgo sobre un Sistema.
Autoridad de Acreditación	Autoridad responsable de la definición y aplicación de la Política STIC.
Autoridad Delegada de Acreditación	Autoridad responsable en su ámbito, de la aplicación de la Política STIC y de las competencias que delegue la AA.
Autoridad Nacional de Seguridad (ANS)	Cargo ejercido conjuntamente por el Ministro de Asuntos Exteriores y el Ministro de Defensa. Su misión es ser el máximo representante de la protección de la información clasificada OTAN/UE/ESA en España. Vela, asimismo, por el cumplimiento de las normas adoptadas en los Acuerdos Bilaterales sucritos por nuestro país en materia de intercambio de materias clasificadas.
Autoridad Nacional de Seguridad-Delegada (ANS-D)	Nombramiento que recae en la persona que ejerce el cargo de Secretario de Estado-Director del CNI. Su misión consiste en ejercer, por delegación, las funciones que le corresponden a la ANS.
Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones	Autoridad designada por el propietario del Sistema, responsable del desarrollo, la operación y mantenimiento del Sistema durante su ciclo de vida; de sus especificaciones, de su instalación y de la verificación de su correcto funcionamiento.
Certificación de la Seguridad	Determinación positiva de que un producto o Sistema tiene capacidad para proteger la información según un nivel de seguridad, y de acuerdo a unos criterios establecidos en el procedimiento o metodología de evaluación correspondiente.
Concepto de Operación	Declaración expresa que realiza la AOSTIC sobre el objeto o función del Sistema, el tipo de información que va a ser manejada, las condiciones de explotación (perfil de seguridad de los usuarios, clasificación de la información, modo de operación, etc.) y las amenazas a las que estará sometido.
Conexión	Se produce una conexión, cuando se proveen los medios físicos y lógicos de transmisión adecuados (por ejemplo enlace satélite, fibra óptica, etc.) susceptibles de ser empleados para el intercambio de información entre Sistemas.
Confidencialidad	Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
Declaración de Requisitos de Seguridad	Es el documento base para la acreditación. Consiste en la exposición completa y detallada de los principios de seguridad que deben observarse y de los requisitos de seguridad que se han de implantar conforme al correspondiente análisis de riesgos realizado previamente.
Disponibilidad	Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.
Evaluación de la Seguridad	Proceso de comprobación de que un producto o Sistema satisface las características de seguridad que proclama tener. Dicho proceso consiste en el examen detallado con el fin de encontrar una posible vulnerabilidad y confirmar el nivel de seguridad establecido. El examen se realiza de acuerdo a un procedimiento o metodología determinado y siguiendo unos criterios de

	evaluación perfectamente definidos y establecidos.
Gestión del Riesgo	Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.
Incidencia	Evento con consecuencias en detrimento de la seguridad.
Integridad	Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
Interconexión	Se produce una interconexión entre Sistemas, cuando existe una conexión y se habilitan flujos de información entre los mismos, con diferentes políticas de seguridad, diferentes niveles de confianza, diferentes Autoridades Operativas de los Sistemas de las Tecnologías de la Información y las Comunicaciones (AOSTIC), o una combinación de las anteriores.
Manejar Información	Presentar, elaborar, almacenar, procesar, transportar o destruir información.
Necesidad de conocer	Determinación positiva por la que se confirma que un posible destinatario requiere el acceso a, el conocimiento de, o la posesión de la información para desempeñar servicios, tareas o cometidos oficiales.
Oficina Nacional de Seguridad (ONS)	Órgano de trabajo de la ANS-D, encargado de la ejecución de sus cometidos.
Órgano de Control	Unidad integrada en la red nacional por la que se recibe, almacena y distribuye información clasificada. Un Órgano de Control puede ser: un Subregistro Principal, o un Punto de Control para la información clasificada procedente de OTAN, UE o ESA, y Servicio de Protección de Información Clasificada en el caso de información clasificada nacional. Cada Órgano de Control cuenta con un Jefe de Seguridad, máximo responsable del cumplimiento de las normas de seguridad.
Procedimientos Operativos de Seguridad	Descripción precisa de la aplicación de los requisitos de seguridad, detallando las responsabilidades y todas las acciones y procedimientos de seguridad a seguir, con el objetivo de garantizar y mantener la seguridad del Sistema. En su caso será la descripción de la aplicación de la DRS correspondiente.
Riesgo	Estimación del grado de exposición de un Sistema frente a amenazas que pudieran causar daños o perjuicios a la Organización.
Seguridad de las Emanaciones o Seguridad TEMPEST	Conjunto de medidas destinadas a evitar fugas de información derivadas de emisiones electromagnéticas no deseadas de equipos electrónicos.
Seguridad de las Tecnologías de la Información y las Comunicaciones	Capacidad de los Sistemas de las Tecnologías de la Información y las Comunicaciones (Sistema) para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, integridad y/o confidencialidad de los datos almacenados o transmitidos y de los servicios que dichos Sistemas ofrecen o hacen accesibles.
Sistema de las Tecnologías de la Información y las Comunicaciones	Conjunto de equipos, métodos, procedimientos y personal, organizado de tal forma que permita almacenar, procesar o transmitir información que está bajo responsabilidad de una única autoridad.
Seguridad Física	Es la condición que se alcanza en las instalaciones cuando se aplica un conjunto de medidas de protección eficaces para la prevención de posibles accesos a información clasificada por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso.
TEMPEST	Término que hace referencia a las investigaciones y estudios de emanaciones comprometedoras (emisiones electromagnéticas no intencionadas, producidas por los equipos eléctricos y electrónicos que, detectadas y analizadas, pueden llevar a la obtención de información) y a las medidas aplicadas para la protección contra dichas emanaciones.

Zona de Acceso Restringido (ZAR)	Local o conjunto de locales en los que, por sus específicas características de seguridad y por el hecho de que en su interior se custodia o maneja información clasificada, se encuentra limitado el acceso en función de parámetros de habilitación de seguridad y/o necesidad de conocer. Deberán contar con las medidas y procedimientos de seguridad adecuados y suficientes, para asegurar la protección de la información clasificada en todo momento.

AA	Autoridad de Acreditación
ADA	Autoridad Delegada de Acreditación
AOSTIC	Autoridad Operativa del Sistema de las Tecnologías de la Información y las Comunicaciones
CC	Criterios Comunes (Common Criteria)
CCN	Centro Criptológico Nacional
CD	Compact Disk
CNI	Centro Nacional de Inteligencia
CO	Concepto de Operación
DVD	Digital Video Disk Digital Versatile Disk
EAL	Evaluation Assurance Level
EGS	Entorno Global de Seguridad
ELS	Entorno Local de Seguridad
ESE	Entorno de Seguridad Electrónica
FTP	File Transfer Protocol
HW	Hardware
IDS	Intrusion Detection System (Sistema de detección de intrusión)
IP	Internet Protocol.
IT	Instrucción Técnica
ITSEC	Information Technology Security Evaluation Criteria
LAN	Local Area Network (red de área local)
OTAN	Organización del Tratado del Atlántico Norte
POC	Point of Contact (punto de contacto)
POS	Procedimientos Operativos de Seguridad
RAM	Random Access Memory
RSA	Responsable de Seguridad del Área
Sistema	Sistema de las Tecnologías de la Información y las Comunicaciones
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SO	Sistema Operativo
SQL	Structured Query Language
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
SW	Software
TCSEC	Trusted Computer Security Evaluation Criteria
TIC	Tecnologías de la Información y las Comunicaciones
WAN	Wide Area Network (red de área extensa)

ANEXO D. REFERENCIAS

[Ref.- 1] Ley 9/1968, de 5 de abril, modificada por ley 48/78, de 7 de octubre sobre Secretos Oficiales.

[Ref.- 2] Decreto 242/1969, de 20 de febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, de 5 de Abril, sobre Secretos Oficiales.

[Ref.- 3] Orden Ministerial Comunicada 1/1982, de 25 de enero, por la que se aprueban las “Normas para la Protección de la Documentación y Material Clasificado”.

[Ref.- 4] Orden Ministerial 76/2002, de 18 de abril, por la que se establece la “Política de Seguridad para la Protección de la Información del Ministerio de Defensa almacenada, procesada o transmitida por sistemas de información y telecomunicaciones.

[Ref.- 5] Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia

[Ref.- 6] Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI)

[Ref.- 7] CCN-STIC-001. Seguridad de los Sistemas de las TIC que manejan información nacional clasificada en la Administración.

[Ref.- 8] CCN-STIC-002. Coordinación Criptológica.

[Ref.- 9] CCN-STIC-003. Uso de cifradores certificados para la protección de información nacional clasificada en la Administración.

[Ref.- 10] CCN-STIC-101. Acreditación de Sistemas de las TIC que manejan información nacional clasificada en la Administración.

[Ref.- 11] CCN-STIC-202. Estructura y contenido de la Declaración de Requisitos de Seguridad (DRS).

[Ref.- 12] CCN-STIC-203. Estructura y contenido de los Procedimientos Operativos de Seguridad (POS).

[Ref.- 13] CCN-STIC-301. Requisitos STIC.

[Ref.- 14] CCN-STIC-302. Interconexión de Sistemas de las TIC que manejan información nacional clasificada en la Administración.

[Ref.- 15] CCN-STIC-430. Herramientas de seguridad.

[Ref.- 16] OR-ASIP-01-02 Orientaciones de Seguridad Física para la protección de la Información Clasificada