RRE117/1: Resolución del Rectorado de la Universidad de Granada por la que se aprueba la modificación de la Política de Seguridad de la Información de la Universidad de Granada

- Resolución del Rectorado de la Universidad de Granada, de 20 de marzo de 2017, por la que se aprueba la modificación de la Política de Seguridad de la Información de la Universidad de Granada

UNIVERSIDAD DE GRANADA

RESOLUCIÓN DEL RECTORADO DE LA UNIVERSIDAD DE GRANADA, DE 21DE MARZO DE 2017, POR LA QUE SE APRUEBA LA MODIFICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE GRANADA

El apartado 10. de la *Política de Seguridad de la información de la Universidad de Granada*, de 18 de septiembre de 2013, establece que será misión del Comité de Seguridad la revisión anual y la propuesta de modificación o mantenimiento de esta *Política de Seguridad de la Información* correspondiendo a la Rectora aprobarla y difundirla.

En cumplimiento del mandato previsto en el mencionado apartado 10. y de acuerdo con el artículo 45 letra u) de los Estatutos de la Universidad de Granada, aprobados por Decreto 231/2011, de 12 de julio (BOJA nº 147, de 28 de julio de 2011) este Rectorado ha resuelto aprobar la propuesta del Comité de Seguridad de modificación de la *Política de Seguridad de la Información* y darle la difusión a través del BOUGR y la web institucional.

Granada, 21 de marzo de 2017

LA RECTORA

Fdo.: Pilar Aranda Ramírez

RESOLUCIÓN DEL RECTORADO DE LA UNIVERSIDAD DE GRANADA, DE 18 de DE SEPTIEMBRE DE 2013, POR LA QUE SE APRUEBA LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE GRANADA

El artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (BOE nº 150, de 23 de junio de 2007), dispone que "El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información".

Por su parte, el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (BOE nº 25, de 29 de enero de 2010), establece como uno de sus pilares fundamentales determinar la política de seguridad que se ha de aplicar en la utilización de los medios electrónicos a los que se refiere la citada Ley 11/2007, de 22 de junio. En concreto, el artículo 11.1 del Real Decreto en cuestión dispone que "Todos los órganos superiores de las Administraciones públicas deberán disponer formalmente de su política de seguridad, que será aprobada por el titular del órgano superior correspondiente".

Por todo cuanto antecede, en cumplimiento del mandato previsto en el mencionado artículo 11.1 y de acuerdo con el artículo 45 letra u) de los Estatutos de la Universidad de Granada, aprobados por Decreto 231/2011, de 12 de julio (BOJA nº 147, de 28 de julio de 2011), **este Rectorado ha resuelto** actualizar la Política de Seguridad de la Información que se anexa.

Granada, 18 de septiembre de 2013

EL RECTOR

Fdo.: Francisco González Lodeiro

UNIVERSIDAD DE GRANADA

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD DE GRANADA

ÍNDICE

1 APROBACIÓN Y ENTRADA EN VIGOR

La Política de Seguridad de la Información se aprueba, con fecha 18 de septiembre de 2013, por el Rector de la Universidad de Granada.

Esta Política es efectiva desde su fecha de aprobación y hasta que sea reemplazada por una nueva Política.

2 INTRODUCCIÓN

La Universidad de Granada considera los sistemas de Tecnologías de Información y Comunicaciones (en adelante TIC) como un elemento de carácter estratégico para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o de los servicios prestados.

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

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y de los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad (en adelante ENS), así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades informadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

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

La entidad debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al artículo 7 del ENS.

2.1 Prevención

Para evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad, la Universidad de Granada implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de las amenazas y riesgos que nos afectan.

Estos controles, y los roles y responsabilidades de seguridad de todo el personal, estarán claramente definidos y documentados.

Para garantizar el cumplimiento de la política, se llevarán a cabo las siguientes actuaciones:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3 Respuesta

La Universidad de Granada:

- Establece mecanismos para responder eficazmente a los incidentes de seguridad.
- Designa punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establece protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, las Unidades, Áreas o Servicios de la Universidad de Granada desarrollarán planes de continuidad de los sistemas TIC como parte de su Plan General de Continuidad del servicio y actividades de recuperación.

3 ALCANCE

Esta Política se aplica a todos los sistemas TIC de la Universidad de Granada y a todos sus miembros, sin excepciones.

4 DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El propósito de esta Política de la Seguridad de la Información es proteger la información y los servicios de la Universidad de Granada.

Es objetivo de esta Institución asegurar que:

- La información y los servicios estén protegidos contra pérdidas de disponibilidad, confidencialidad e integridad.
- La información esté protegida contra accesos no autorizados.
- Se cumplan los requisitos legales aplicables.
- Se cumplan los requisitos del servicio respecto a la seguridad de la información y los sistemas de información.
- Las incidencias de seguridad sean comunicadas y tratadas apropiadamente.
- Se establezcan procedimientos para cumplir con esta Política.
- El Responsable de Seguridad de la Información sea el encargado de mantener esta Política, los procedimientos y de proporcionar apoyo en su implementación.
- El Responsable de Servicio sea el encargado de implementar esta Política y sus correspondientes procedimientos.
- Cada empleado sea responsable de cumplir esta Política y sus procedimientos según aplique a su puesto.
- La Universidad de Granada implemente, mantenga y realice un seguimiento del cumplimiento del Esquema Nacional de Seguridad.

5 MARCO NORMATIVO

Según la legislación vigente, las leyes aplicables a la Universidad de Granada en materia de Seguridad de la Información son:

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica (BOE de 29 de enero de 2010).
- Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.
- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (BOE de 14 de diciembre de 1999).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (BOE de 19 de enero de 2008).
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual (BOE de 22 de abril de 1996).
- Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público (BOE de 13 de abril de 2007).

La Universidad de Granada cumple con la legislación citada y con todos sus requisitos.

Las otras leyes, reglamentos y normativa, nacional o internacional, a la que la Universidad de Granada está sujeto son:

Legislación básica sobre universidades a nivel estatal

- Ley Orgánica 6/2001, de 21 de diciembre de Universidades (BOE de 24 de diciembre de 2001).
- Ley Orgánica 4/2007, de 12 de abril, por la que se modifica la Ley Orgánica 6/2001 de 21 de diciembre de Universidades (BOE de 13 de abril de 2007).

Legislación básica sobre acceso a estudios universitarios

- Real Decreto 412/2014, de 6 de junio, por el que se establece la normativa básica de los procedimientos de admisión a las enseñanzas universitarias oficiales de Grado (BOE de 7 de junio de 2014)

Legislación básica sobre estudios universitarios

- Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales (BOE de 30 de octubre de 2007).
- Real Decreto 1509/2008, de 12 de septiembre, por el que se regula el Registro de Universidades, Centros y Títulos (BOE de 25 de septiembre de 2008).
- Real Decreto 1002/2010, de 5 de agosto, sobre expedición de títulos universitarios oficiales
- Real Decreto 99/2011, de 28 de enero, por el que se regulan las enseñanzas oficiales de doctorado (BOE de 10 de febrero de 2011).
- Real Decreto 22/2015, de 23 de enero, por el que se establecen los requisitos de expedición del Suplemento Europeo a los títulos regulados en el Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales y se modifica el Real Decreto 1027/2011, de 15 de julio, por el que se establece el Marco Español de Cualificaciones para la Educación Superior
- Real Decreto 195/2016, de 13 de mayo, por el que se establecen los requisitos para la expedición del Suplemento Europeo al Título Universitario de Doctor

Ley Andaluza de Universidades

- Decreto Legislativo 1/2013, de 8 de enero, por el que se aprueba el texto refundido de la Ley Andaluza de Universidades (BOJA de 11 de enero de 2013).

6 ORGANIZACIÓN DE LA SEGURIDAD

6.1 Comité: Composición y Funciones

El Comité de Seguridad de la Información coordina la seguridad de la información en la Universidad de Granada.

El Comité de Seguridad de la Información estará presidido por la persona titular de la Secretaría General y formado por:

- Responsable de la Información, la persona titular de la Secretaría General de la UGR, en nombre y representación de ella o persona en quien delegue.
- Responsable de los Servicios, la persona titular de la Gerencia o persona en quien delegue.
- Responsable de Seguridad, la persona titular de la Dirección del Centro de Servicios de Informática y Redes de Comunicaciones.
- Responsable del Sistema, la persona titular de la Subdirección del Centro de Servicios de Informática y Redes de Comunicaciones.
- Delegado de la Rectora para la Universidad Digital o, en su caso, persona que ostente dichas competencias.

El Comité de Seguridad tendrá las siguientes funciones:

- Informar regularmente del estado de la seguridad de la información al Rectorado.
- Promover la mejora continua del sistema de gestión de la seguridad de la información.
- Elaborar la estrategia de evolución de la Universidad de Granada en lo que respecta a seguridad de la información.
- Coordinar los esfuerzos de las diferentes áreas en materia de seguridad de la información, para asegurar que los esfuerzos son consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.
- Elaborar y revisar regularmente la Política de Seguridad de la Información para que sea aprobada por el Rector.
- Aprobar la normativa de seguridad de la información.

- Elaborar y aprobar los requisitos de formación y calificación de administradores, operadores y usuarios desde el punto de vista de seguridad de la información.

- Monitorizar los principales riesgos residuales asumidos por la Universidad de Granada y recomendar posibles actuaciones respecto de ellos.

- Monitorizar el desempeño de los procesos de gestión de incidentes de seguridad y recomendar posibles actuaciones respecto de ellos. En particular, velar por la coordinación de las diferentes áreas de seguridad en la gestión de incidentes de seguridad de la información.

- Promover la realización de las auditorías periódicas que permitan verificar el cumplimiento de las obligaciones del organismo en materia de seguridad.

- Aprobar planes de mejora de la seguridad de la información de la Universidad de Granada En particular velará por la coordinación de diferentes planes que puedan realizarse en diferentes áreas.

- Priorizar las actuaciones en materia de seguridad cuando los recursos sean limitados.

- Velar porque la seguridad de la información se tenga en cuenta en todos los proyectos TIC desde su especificación inicial hasta su puesta en operación. En particular deberá velar por la creación y utilización de servicios horizontales que reduzcan duplicidades y apoyen un funcionamiento homogéneo de todos los sistemas TIC.

- Resolver los conflictos de responsabilidad que puedan aparecer entre los diferentes responsables, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

El Secretario del Comité de Seguridad será el Responsable de Seguridad y tendrá como funciones:

- Convocar, según las indicaciones de la presidencia, las reuniones del Comité de Seguridad de la Información.

- Preparar los temas a tratar en las reuniones del Comité, aportando información puntual para la toma de decisiones.

- Elaborar el acta de las reuniones.

- Llevar a cabo la ejecución directa o delegada de las decisiones del Comité.

6.2 Funciones de los miembros del Comité

Las funciones de los miembros del Comité de Seguridad de la Información serán las siguientes:

Responsable de la Información

- Velar por el buen uso de la información y, por tanto, de su protección.
- Ser responsable último de cualquier error o negligencia que lleve a un incidente de confidencialidad o de integridad.
- Establecer los requisitos de la información en materia de seguridad.
- Determinar los niveles de seguridad de la información.

Responsable de los Servicios

- Establecer los requisitos del servicio en materia de seguridad, incluyendo los correspondientes a interoperabilidad, accesibilidad y disponibilidad.
- Determinar los niveles de seguridad de los servicios.

Responsable de Seguridad

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad.
- Promover la formación y concienciación en materia de seguridad de la información.

Responsable del Sistema

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Definir la topología y sistema de gestión del Sistema de Información estableciendo los criterios de uso y los servicios disponibles en el mismo.
- Cerciorarse de que las medidas específicas de seguridad se integren adecuadamente dentro del marco general de seguridad.

7 FUNCIONES DE LOS ADMINISTRADORES DE LA SEGURIDAD DE LOS SISTEMAS

Los Jefes de Servicio del Centro de Servicios de Informática y Redes de Comunicaciones relacionados con la materia, en calidad de Administradores de la Seguridad de los Sistemas, tendrán las siguientes funciones:

- Implementar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información.
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información.
- Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.
- Aplicar los Procedimientos Operativos de Seguridad.
- Aprobar los cambios en la configuración vigente del Sistema de Información.
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente.
- Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.
- Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.
- Informar al Responsable de la Seguridad y Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

8 RESOLUCIÓN DE CONFLICTOS

De acuerdo con el Principio de Jerarquía que rige en las administraciones públicas españolas, en caso de conflicto entre los diferentes responsables y/o entre diferentes servicios

de la entidad, éste será resuelto por el superior jerárquico de los mismos. En defecto de lo anterior, prevalecerá la decisión del Comité de Seguridad, elevando aquellos casos en los que no tenga suficiente autoridad para decidir.

9 PROCEDIMIENTOS DE DESIGNACIÓN

El Rector designará al Responsable del Seguridad y al Responsable de Sistema, a propuesta del Comité de Seguridad, precisando sus funciones y responsabilidades dentro del marco establecido por esta Política. La designación se revisará cada dos años o cuando el puesto quede vacante.

10 REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del Comité de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de modificación o mantenimiento de la misma. La Política será aprobada por el Rector y difundida para que la conozcan todas las partes afectadas.

11 GESTIÓN DE DOCUMENTACIÓN DEL SGSI

Todos los documentos que componen la documentación del Sistema de Gestión de Seguridad de la Información se gestionarán de acuerdo a lo descrito en el procedimiento de seguridad de gestión del SGSI.

12 DATOS DE CARÁCTER PERSONAL

La Universidad de Granada trata datos de carácter personal. El Documento de Seguridad, que se puede encontrar en la Secretaría General, recoge, entre otros aspectos, los ficheros inscritos en la Agencia Española de Protección de Datos y los responsables correspondientes. Todos los sistemas de información de la Universidad de Granada se ajustarán a los niveles de seguridad requeridos por la normativa en materia de protección de datos, en función de la naturaleza y finalidad de los datos de carácter personal recogidos en el mencionado Documento de Seguridad.

Cuando se traten datos personales en la información, la Política de Seguridad de la Información complementa las políticas de seguridad de la Universidad de Granada en materia de protección de datos de carácter personal.

13 GESTIÓN DE RIESGOS

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

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

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

La gestión de riesgos quedará documentada en el Informe de Análisis y Gestión de Riesgos.

14 POLÍTICA DE USO ACEPTABLE

Los sistemas de información y la información serán utilizados únicamente para los fines y propósitos para los que han sido puestos a disposición de los usuarios.

Las usos aceptables se recogen en la "Normativa de uso de los recursos informáticos", que se pone a disposición de todos los usuarios de los servicios de la UGR en http://biblioteca.ugr.es/pages/biblioteca_ugr/normativa/normativa_recursos_informaticos

15 DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Política de Seguridad de la Información se desarrollará por medio de Normativa de Seguridad que afronte aspectos específicos. La Normativa de Seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La Normativa de Seguridad estará disponible en la intranet para su consulta.

16 OBLIGACIONES DEL PERSONAL

Todo el personal de la Universidad de Granada tiene la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Comité de Seguridad disponer los medios necesarios para que la información llegue a los afectados.

Todo el personal relacionado con la información y los sistemas de la Universidad de Granada recibirá formación en seguridad de la información. Se establecerá un programa de concienciación continua para atender a todo el personal de la Universidad de Granada, en particular a los de nueva incorporación.

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

17 TERCERAS PARTES

Cuando la Universidad de Granada preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipe de esta Política de Seguridad de la Información, se establecerán canales para informe y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando la Universidad de Granada utilice servicios de terceros o ceda información a terceros, se les hará partícipe de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en la mencionada Normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de informe y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se detalla en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos.