NOMBRE DEL DOCUMENTO:

Política sobre Seguridad de Información

	NOMBRE	PUESTO
APROBADO POR	**Marcela Aguilar**	Director de Administración y Finanzas CSC
	Mario Quintanar Salinas	Gerente de Procesos y TI
REVISADO POR	**Oliverio Rodríguez**	Coordinador de Seguridad de Información
	Juan Manuel Ocañas Mireles	Coordinador de Procesos de Negocio
ELABORADO POR	**Rodolfo Delgado Monsivais**	Consultor de Procesos de Negocio

TABLA DE CONTENIDOS

GENERALIDADES

Objetivo

Dar a conocer las Políticas, Lineamientos y Procedimientos a seguir en Grupo Delta referentes a la Seguridad de Información, los cuales deberán estar basadas en el cumplimiento de las regulaciones aplicables y a los marcos de referencia y estándares internacionales en la materia.

Alcance

Todos los Colaboradores contratados por Grupo Delta, así como el personal externo (outsourcing y proveedores) que tenga acceso a los recursos Tecnológicos o a los sistemas, deberán apegarse a las Políticas, lineamientos y procedimientos internos de Grupo Delta.

INTRODUCCIÓN

Dentro de Grupo Delta se establecen los lineamientos y políticas aplicables a la Seguridad de la información. La información es un activo que es esencial para cualquier institución y en consecuencia necesita ser protegido adecuadamente. Como resultado de una creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y a una variedad más amplia de amenazas y vulnerabilidades.

La información puede existir en muchas formas, puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

POLÍTICAS GENERALES

1. PAPEL DE LA INFORMACIÓN Y DE LOS SISTEMAS DE INFORMACIÓN

- Grupo Delta depende de manera decisiva de la información y de los sistemas de información. Si se divulgara información importante a las personas inadecuadas, la empresa podría sufrir serias pérdidas. La

buena reputación de la cual disfruta Grupo Delta además está directamente relacionada con la forma en que maneja la información y los sistemas de información. Por ejemplo, si se divulgara públicamente información privada del cliente, se dañaría la reputación de la organización.

2. ESFUERZO EN EQUIPO

- Para ser eficaz, la seguridad de la información debe consistir en un esfuerzo en equipo que incluya la participación y el apoyo de cada colaborador de Grupo Delta que se ocupe de la información y los sistemas de información. En reconocimiento a la necesidad de trabajo en equipo, esta Política aclara las responsabilidades de los usuarios y los pasos que deben seguir para ayudar a proteger la información y los sistemas de información de Grupo Delta. Este documento describe las formas de evitar y responder ante diversas amenazas a la información y a los sistemas de información incluido el acceso no autorizado, la divulgación, la duplicación, la modificación, la apropiación, la destrucción, la pérdida, el uso indebido y la negación de uso.

3. PERSONAS INVOLUCRADAS

- Cada colaborador de Grupo Delta debe cumplir con las Políticas de seguridad de la información que se encuentran en este y en los documentos de seguridad de información relacionados. Los colaboradores que contravengan en forma deliberada esta Política de seguridad de información u otras declaraciones serán sometidos a medidas disciplinarias.

4. SISTEMAS INVOLUCRADOS

- Esta política se aplica a todos los sistemas computacionales y de redes de propiedad de Grupo Delta o administrados por ésta. Esta política se aplica a todos los sistemas operativos, equipos de cómputo y sistemas de aplicaciones. Esta política cubre sólo la información que manejan las computadoras y las redes. Aunque este documento incluye una mención de otras manifestaciones de información, como la verbal y la impresa, no aborda directamente la seguridad de la información en estas formas.

5. TRES CATEGORIAS DE RESPONSABILIDADES

- Para coordinar el esfuerzo en equipo, Grupo Delta ha establecido tres categorías, de las cuales, por lo menos una se aplica a cada colaborador. Estas categorías son Propietario, Custodio y Usuario. Estas categorías definen responsabilidades generales con respecto a la seguridad de la información.

5.1 Responsabilidades de los propietarios

Toda información del sistema de aplicaciones de producción debe tener un Propietario designado. Para cada tipo de información, los Propietarios designan la clasificación de sensibilidad pertinente, designan el nivel adecuado de criticalidad, definen a cuáles usuarios se les otorgará acceso y aprueban las solicitudes para las diversas formas en que se utilizará la información.

5.2 Responsabilidades de los custodios

Los custodios se encuentran en posesión física o lógica de información de Grupo Delta o información confiada a Grupo Delta. Los custodios son responsables de salvaguardar la información, incluida la implementación de sistemas de control de acceso para evitar la divulgación inadecuada, y realizar copias de seguridad, de modo de que no se pierda información fundamental. Los custodios deben implementar, manejar y mantener las medidas de seguridad definidas por los Propietarios de la información.

5.3 Responsabilidades de los usuarios

Los usuarios son responsables de familiarizarse y cumplir con todas las políticas, procedimientos y normas de Grupo Delta que se relacionan con seguridad de la información. Las preguntas sobre el manejo adecuado del tipo específico de información se deben dirigir al Custodio o al Propietario de la información involucrada.

6. MANEJO DE INFORMACIÓN CONSECUENTE

- Se debe proteger la información de Grupo Delta o la información que se ha confiado a Grupo Delta de manera proporcional a su sensibilidad y criticalidad. Se deben emplear medidas de seguridad sin importar los medios en que se almacene la información, los sistemas que la procesen o los métodos mediante los cuales ésta se traslade. Se debe proteger la información de manera que sea consecuente con su clasificación.

7. ADMINISTRACIÓN DE CONTRASEÑAS

7.1 Indicadores de usuarios y contraseñas

Grupo Delta requiere que cada colaborador que tiene acceso a los sistemas de información para múltiples usuarios tenga un identificador de usuario único y una contraseña privada. Se deben emplear estos identificadores de usuario para restringir los privilegios del sistema basándose en los deberes del cargo, responsabilidades del proyecto y otras actividades del negocio. Cada colaborador es personalmente responsable por la utilización de su identificador de usuario y contraseña.

7.2 Identificadores de usuarios anónimos

Con la excepción de sitios de Internet y otros sistemas en que se tiene la intención de que todos los usuarios normales sean anónimos, se prohíbe a los usuarios iniciar sesión en cualquier sistema o red de Grupo Delta en forma anónima. Por ejemplo, el acceso anónimo podría incluir el uso de identificadores de usuario "invitado". Cuando los usuarios emplean comandos del sistema que les permiten cambiar los identificadores de usuario activos para obtener ciertos privilegios, inicialmente deben haber iniciado sesión empleando identificadores de usuario que indicaban en forma clara sus identidades.

7.3 Contraseñas difíciles de adivinar

Los usuarios deben seleccionar contraseñas que sean difíciles de adivinar. Esto significa que las contraseñas no deben estar relacionadas con el trabajo o la vida personal individual. Por ejemplo, no se debe usar el número de matrícula del automóvil, nombre del cónyuge, ni fragmentos de una dirección. Esto además significa que las contraseñas no deben ser una palabra encontrada en el diccionario ni alguna otra parte de la oración. Por ejemplo, no se deben usar nombres propios, lugares, términos técnicos ni jerga.

7.4 Contraseñas fáciles de recordar

Los usuarios pueden seleccionar contraseñas fáciles de recordar que al mismo tiempo resulten difíciles de adivinar para las personas no autorizadas.

- Unas varias palabras
- Desplace los caracteres de una palabra alguna cantidad de letras hacia delante o atrás en el alfabeto
- Transforme una palabra normal según un método específico, como convertir en forma alternada cada letra en un número que refleje su posición en la palabra.

- Combine la puntuación o los números con una palabra normal
- Cree siglas con las palabras de una canción, poema u otra secuencia conocida de palabras
- Deletree incorrectamente una palabra en forma intencional
- Combine varias preferencias, como las horas de sueño deseadas y los colores favoritos.

7.5 Patrones de contraseñas repetidos

Los usuarios no deben crear contraseñas con una secuencia básica de caracteres que se cambie parcialmente basándose en la fecha o en algún factor predecible. Los usuarios no deben crear contraseñas que sean idénticas o significativamente similares a las contraseñas que haya usado el colaborador con anterioridad.

7.6 Restricciones de las contraseñas

Las contraseñas deben tener por lo menos 12 caracteres de longitud. Éstas se deben cambiar cada 60 días o con mayor frecuencia. Cada vez que un colaborador sospeche que otra persona conoce una contraseña, ésta se debe cambiar de inmediato.

7.7 Almacenamiento de contraseñas

Las contraseñas no se deben almacenar en forma legible en archivos por lotes, secuencias de comandos de inicio de sesión automático, macros de software, teclas de función de terminal, computadoras sin sistemas de control de acceso o en otros lugares en que personas no autorización podrían descubrirlas. No se deben escribir las contraseñas en alguna forma fácil de descifrar ni dejarse en un lugar en que personas no autorizadas podrían descubrirlas.

7.8 Compartir contraseñas

Si los colaboradores necesitan compartir datos residentes en computadoras, deben usar correo electrónico, bases de datos de groupware, directorios públicos en servidores de redes de área local, intercambio manual de disquetes y otros mecanismos. Aunque se compartan los identificadores de usuarios para correo electrónico u otros propósitos, nunca se deben compartir con otros las contraseñas ni revelarlas. La única vez en que una contraseña debe ser conocida por otra persona es cuando se emite. Estas contraseñas temporales se deben cambiar la primera vez que el usuario autorizado accede al sistema. Si un usuario cree que otra persona está usando su identificador de

usuario y contraseña, éste debe notificar de inmediato al área de Tecnóloga de la Información mediante la plataforma de Service Desk < https://serviciosti.ddelta.mx >.

8. EMISION DE INFORMACION A TERCEROS

- A menos que se designe específicamente como pública, toda la información interna de Grupo Delta se debe proteger de la divulgación a terceros. Es posible que se otorgue acceso a información interna de Grupo Delta a terceros sólo cuando exista una necesidad de saber demostrable, cuando se haya firmado un acuerdo de no divulgación (NDA) de Grupo Delta, y cuando el Propietario de información de Grupo Delta pertinente haya autorizado explícitamente tal divulgación. Si se pierde información sensible, se divulga a personas no autorizadas o se sospecha que se ha perdido o divulgado a personas no autorizadas, se deberá notificar al Propietario de la información y al departamento de Seguridad de la Información.

9. POLITICA DE ESCRITORIOS LIMPIOS Y PANTALLAS DESPEJADAS

- Los colaboradores de Grupo Delta deberán:
  a. Almacenar la información sensible en gabinetes adecuados bajo llave y/o alguna otra forma de muebles de seguridad.
  b. Asegurar las estaciones de trabajo usando mecanismos de cables de seguridad o de cierre de acoplamiento, guardadas en gabinetes bajo llave y/o alguna otra forma de muebles de seguridad.
  c. Establecer una contraseña para el encendido.
  d. Establecer una contraseña para la unidad de disco duro (si está disponible)
  e. Establecer una contraseña del protector de pantalla para bloquear la pantalla si se encuentra inactiva por 5 minutos
  f. Cerrar la sesión de las estaciones de trabajo y terminales computacionales cuando se encuentren sin supervisión
  g. Recoger la información confidencial de las impresoras de inmediato

10. ACCESO A INTERNET

- Los colaboradores disponen de acceso a Internet para desempeñar sus deberes laborales, pero este acceso podría terminarse en cualquier momento a discreción. Se supervisa el acceso a Internet para asegurarse de que los colaboradores no visiten sitios que no se relacionen con sus empleos y también para

asegurarse de que continúen cumpliendo con las políticas de seguridad. Los colaboradores deben tener especial cuidado de asegurarse de no representar a Grupo Delta en los grupos de discusión ni en otros foros públicos, a menos que previamente hayan recibido autorización de la administración superior para actuar con esta facultad. Se debe considerar sospechosa toda la información recibida de Internet hasta que la hayan confirmado fuentes fidedignas. Los colaboradores no deben colocar material de Grupo Delta ni ningún sistema computacional públicamente accesible, como Internet, a menos que la exposición haya sido aprobada por el Propietario de la información. No se debe enviar a través de Internet información sensible, como contraseñas y números de tarjetas de crédito, a menos que esta información se encuentre en forma cifrada.

11. DISPOSITIVOS DE ALMACENAMIENTO EXTRAIBLES

- El término" dispositivos de almacenamiento extraíble" se refiere a todo aquel dispositivo periférico que pueda utilizarse para almacenar información, con el cual sea susceptible a fuga de la misma, o intrusión de código malicioso, a acceder al equipo de cómputo por medio de aplicaciones que se puedan instalar en segundo plano con el cual se pueda vulnerar las políticas de la empresa, etc.

- Algunos de los lineamientos que grupo delta deberá cumplir son los siguientes:
  a. Los equipos de cómputo de Grupo Delta deben contar con una configuración por defecto, que no le sea posible al usuario utilizar dispositivos de almacenamiento extraíble, a menos de que solicite este privilegio de manera formal y cuente con las autorizaciones previstas en el presente.
  b. Los privilegios para habilitar los dispositivos de almacenamiento extraíble se otorgarán únicamente con las debidas autorizaciones y de acuerdo con las políticas y procedimientos establecidos por Grupo Delta, siempre y cuando exista la necesidad operativa o de entrega de información a alguna autoridad externa, clientes, accionistas y/o proveedores.
  c. Todos los equipos que se encuentren expuestos en las diferentes unidades de negocio y en un esquema de teletrabajo, deberán tener inhabilitado el acceso a dispositivos de almacenamiento extraíble.

12. SEGURIDAD DE LOS EQUIPOS MOVILES

- El uso de cualquier equipo para procesamiento de información de grupo delta fuera de sus instalaciones debe ser autorizado por el área de seguridad de la información. La seguridad utilizada debe ser equivalente a la empleada en equipo interno para el mismo propósito, tomando en cuenta el riesgo de trabajar fuera de las instalaciones.

- Se considerarán al menos los siguientes controles:

d. Los equipos y periféricos que salgan de las instalaciones no deben ser desatendidos en lugares públicos.
e. En caso de viajes, las computadoras portátiles deben ser transportadas como equipaje de mano.
f. Cuando sean transportadas en un automóvil, deberán ser transportadas de preferencia en la cajuela del vehículo.

13. TELETRABAJO

- El teletrabajo utiliza tecnología de comunicaciones para permitir que el Colaborador labore desde una ubicación fuera de Grupo Delta. La protección apropiada del lugar de trabajo remoto deberá ser contra robo de equipo e información, contra uso no autorizado de información, contra acceso remoto no autorizado a los sistemas internos de Grupo Delta o el mal uso de los Sistemas de Grupo Delta.

- Se deberán considerar al menos los siguientes controles:
  a. La existencia de seguridad física del lugar de trabajo remoto.
  b. La seguridad de las comunicaciones, tomando en consideración la necesidad de acceso remoto a los sistemas internos de Grupo Delta.
  c. La amenaza de accesos no autorizados a la información o recursos por otra gente en el lugar remoto, por ejemplo, familiar o amigos.
  d. La disponibilidad de equipo y mobiliario de almacenaje apropiado para las actividades de trabajo remoto.
  e. Métodos para asegurar accesos remotos seguros (VPN).

14. CORREO ELECTRONICO Y PLATAFORMAS DE COLABORACION

- Los usuarios deben comprender que:
  a. El correo electrónico y plataformas de colaboración se usará para propósitos autorizados por Grupo Delta.
  b. La información almacenada sobre estas plataformas son propiedad de Grupo Delta.
  c. No se permitirán correos electrónicos que incluyan opinión no fundamentada, sexista, racista u otro material potencialmente ofensivo en el contenido

- El Correo Electrónico, así como las Plataformas de colaboración deberán ser usados solamente para los propósitos del negocio, los Colaboradores no deberán tener expectativas de privacidad y propiedad personal asociada a la información que guarden o almacenen a través de estas plataformas.

- Queda prohibido las siguientes acciones:

a. Participar en mensajes del tipo cadena.
b. Prestar la cuenta de correo electrónico a otra persona o usar el correo electrónico de otro colaborador.
c. Almacenar información de carácter personal, dentro de las plataformas. (fotografías, música, documentación personal diversa, etc.).

- Para mantener y administrar de manera adecuada esta propiedad, éste se reserva el derecho de examinar y verificar todos los datos que se almacenen o se transmitan. Esta política es pertinente a todas las cuentas de correo electrónico (interno, externo, genérico y servicios). Se aplicará una medida disciplinaria para las fallas o uso inadecuado.

15. ANALISIS DE MALWARE

- Todos los usuarios deben mantener activas en sus equipos las versiones actuales del software de análisis de malware aprobado. Los usuarios no deben anular los procesos automáticos del software que actualizan las firmas de malware. Se debe usar software de detección de malware para analizar todo el software y los archivos de datos provenientes de terceros o de otros grupos de Grupo Delta. Se debe realizar este análisis antes de abrir nuevos archivos de datos y antes de ejecutar un nuevo software. Los colaboradores no deben omitir o desactivar los procesos de análisis que podrían evitar la transmisión de malware informáticos.

16. ERRADICACION DE MALWARE INFORMATICOS

- Si los colaboradores sospechan de una infección de un malware informático, inmediatamente deberán dejar de usar la computadora involucrada y contactar al área de Tecnologías de la Información mediante la plataforma de Service Desk < https://serviciosti.ddelta.mx >. Además, la computadora infectada se debe aislar de inmediato de las redes internas.

17. FUENTES DE SOFTWARE

- Las computadoras y redes de Grupo Delta no deben ejecutar software que provenga de fuentes que no sean los departamentos de Grupo Delta, grupos de usuarios informados y confiables, autoridades de seguridad de seguridad de sistemas bien conocidos o proveedores de computadoras, redes o software comercial establecidos. No se debe usar el software descargado de dominio público y otro software de

fuentes no confiables, a menos que se haya sometido a un riguroso régimen de pruebas que haya aprobado el Departamento de Tecnología de la Información.

18. CONTROL DE CAMBIOS FORMAL

- Todos los sistemas computacionales y de comunicaciones usados para el procesamiento de la producción deben seguir el proceso de Control de Cambios usado para asegurar que sólo se realicen cambios autorizados. Se debe usar este procedimiento de control de cambios para todos los cambios significativos al software, hardware, vínculos de comunicaciones y procedimientos del sistema de producción.

19. CONVENCIONES DE DESAROLLO Y SISTEMAS

- Todas las actividades de desarrollo del software de producción y de mantenimiento de software realizadas por el personal interno deben cumplir con las políticas, normas, procedimientos y otras convenciones de desarrollo de sistemas del departamento de Tecnología de la Información. Estas convenciones incluyen las pruebas, capacitación y documentación adecuadas. Para obtener más información sobre este tema, consulte “GD-P-AYF-TI-SIT-001 Política sobre Seguridad de Información”.

20. LICENCIAS ADECUADAS

- La administración de Grupo Delta debe tomar las medidas pertinentes con los proveedores de software para obtener copias autorizadas adicionales, siempre y cuando se necesiten copias adicionales para las actividades comerciales. Todo el software se debe ser aprobado por Tecnología de la Información.

21. COPIAS NO AUTORIZADAS

- Los usuarios no deben copiar el software proporcionado por Grupo Delta en ningún medio de almacenamiento, no deben transferir dicho software a otra computadora ni divulgar dicho software a personas externas sin la autorización previa de su supervisor. Copias de seguridad regulares son una excepción autorizada a esta política.

22. RESPONSABILIDAD DE COPIA DE SEGURIDAD DE LA INFORMACION EN LAPTOPS

- El colaborador tiene la responsabilidad de asegurarse que la información con la que desempeña sus funciones dentro de Grupo Delta se encuentre resguardada de manera adecuada.
- Se considerarán al menos los siguientes controles:
  a. El colaborador deberá resguardar toda su información de Grupo Delta dentro de la Nube de Microsoft Office 365.
  b. El servicio de Nube que se utilizara es Microsoft One Drive.

23. DIVULGACIÓN EXTERNA DE INFORMACIÓN DE SEGURIDAD

- La información acerca de las medidas de seguridad para los sistemas computacionales y de redes de Grupo Delta es confidencial y no se debe difundir a aquellos que son usuarios no autorizados de los sistemas involucrados.

24. DERECHOS DE MATERIAL DESARROLLADO

- Mientras prestan servicios a Grupo Delta, los colaboradores otorgan a Grupo Delta los derechos exclusivos de las patentes, derechos de autor, invenciones u otra propiedad intelectual que originen o desarrollen. Todos los programas y documentación generada o proporcionada por los colaboradores para beneficio de Grupo Delta son propiedad de Grupo Delta. Grupo Delta determina la propiedad legal de los contenidos de todos los sistemas de información bajo su control. Grupo Delta se reserva el derecho de evaluar y usar esta información a su discreción.

25. DERECHO A BUSCAR Y SUPERVISAR

- Grupo Delta se reserva el derecho de supervisar, inspeccionar o buscar en cualquier momento todos los sistemas de información de Grupo Delta. Este examen podría realizarse con o sin el consentimiento, presencia, o conocimiento de los colaboradores involucrados. Los sistemas de información sujetos a tal examen incluyen, pero sin limitación, archivos del sistema de correo electrónico, archivos del disco duro de computadoras, archivos de correos de voz, archivos de cola de impresora, cajones de escritorio y áreas de almacenamiento. Todas las búsquedas de esta naturaleza se deberán realizar después de obtener la aprobación de los departamentos Auditoría Interna, Recursos Humanos y de Seguridad de la información.

El área de Tecnologías de la Información de Grupo Delta se reserva el derecho de eliminar de sus sistemas de información cualquier material que considere ofensivo o potencialmente ilegal.

26. USO PERSONAL

- Los sistemas de información de Grupo Delta tienen el objetivo de usarse sólo para fines comerciales. Se permite un uso personal secundario si éste no consume más que una cantidad insignificante de recursos que de otro modo se podrían usar para fines comerciales, no interfiere con la productividad de los colaboradores y no impide ninguna actividad comercial. Por ejemplo, un uso secundario permitido de un sistema de correo electrónico comprendería el envío de un mensaje para programar un almuerzo. Se prohíbe el uso de sistemas de información para cartas de cadenas, solicitud de beneficencia, material de campañas políticas, trabajo religioso, transmisión de material censurable u otro uso no comercial.

27. HERRAMIENTAS QUE COMPROMETEN LA SEGURIDAD

- Salvo que el departamento de Seguridad de la Información lo autorice específicamente, los colaboradores de Grupo Delta no deben adquirir, poseer, comerciar o usar herramientas de hardware o software que se podrían usar para evaluar o comprometer la seguridad de los sistemas de información. Ejemplos de tales herramientas incluyen aquellas que desactivan la protección contra copia de software, descubren contraseñas secretas, identifican vulnerabilidades de seguridad o descifran archivos cifrados. Sin este tipo de aprobación, se prohíbe a los colaboradores usar cualquier hardware o software que supervise el tráfico de una red o la actividad de una computadora.

28. ACTIVIDADES PROHIBIDAS

- Los usuarios no deben probar ni intentar comprometer las medidas de seguridad del sistema computacional o de comunicaciones a menos que esto sea específicamente aprobado por anticipado y por escrito por el área de Seguridad de la Información. Los incidentes que incluyen piratería del sistema, adivinanza de contraseñas, descifrado de archivos, copia de software pirata sin aprobación, o intentos no autorizados similares de comprometer las medidas de seguridad podrían ser ilegales y se considerarán serias contravenciones a la política interna de Grupo Delta. Se prohíbe estrictamente los accesos directos que evaden las medidas de seguridad de los sistemas y hacer bromas que comprometan las medidas de seguridad de los sistemas.

29. INFORMACIÓN OBLIGATORIA

- Se debe informar de inmediato al área de Seguridad de información <orodriguez@gdelta.mx > de todas las sospechas de contravenciones a la política, intrusiones al sistema y otras condiciones que podrían amenazar la información de Grupo Delta o los sistemas de información de Grupo Delta.

SANCIONES

Cualquier punto no considerado en la presente política será canalizado con el Comité de Ética quien definirá las acciones a seguir, a fin de evitar cualquier juicio personal.

En caso de faltas a la Política, la persona será acreedora a una sanción por parte del Comité de Ética quien valorará la posible desviación y aplicará una amonestación por la causa, validando si fue en forma dolosa o culposa por el acto señalado.

MARCO NORMATIVO

- Norma ISO 27001:2022

CONTROL CAMBIOS

Fecha de emisión	Fecha de actualización	Próxima revisión	Versión	Descripción del cambio
04/10/2021	N/A	31/12/2021	Versión 1.0	Documento inicial de nueva creación.
13/08/2022	13/08/2022	31/12/2022	Versión 2.0	Actualización.
01/05/2023	14/04/2023	31/12/2023	Versión 3.0	Actualización. Sustituye al documento **GD-CIS-PO-001** Políticas Aplicables a la Seguridad de la Información

FORMATOS, REFERENCIAS Y ANEXOS

N/A

[RESTO DE LA PÁGINA INTENCIONALMENTE EN BLANCO)