PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Departamento de Comunicaciones (CEDE6)

2023

Control de cambios		
Fecha	Versión	Descripción
22/12/2022	1.0	Creación

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Las medidas preventivas y reactivas en los sistemas tecnológicos para la seguridad de la información, permiten resguardar y proteger la información ante amenazas o brechas que vayan en contra de los principios de confidencialidad, integridad y disponibilidad de la información. Además, mediante la implementación de medidas de control se pueden gestionar y reducir los riesgos e impactos que afecten la información institucional.

Por consiguiente, el presente plan se elabora con el fin de dar a conocer cómo se realizará la gestión y socialización de los riesgos asociados a la seguridad de la información, con la finalidad de proteger los datos e información institucional, así como para dar cumplimiento a la normativa establecida por el Estado colombiano, en especial del documento CONPES 3995 de 2020, “Confianza y Seguridad Digital”, el Decreto 767 de mayo de 2022, “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital para Colombia y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones” y el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Adicionalmente, se tienen en cuenta las buenas prácticas y los lineamientos de los estándares NTC-ISO/IEC 27001:2013 y la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, del Departamento Administrativo de la Función Pública (DAFP).

2. DEFINICIONES

- **Activo:** “En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización” (ISO/IEC 27000:2018).

- **Archivo:** “Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, y que se encuentran conservados respetando un orden definido, para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura” (Ley 594 de 2000 art 3).

- **Amenaza:** “Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización” (ISO/IEC 27000:2018).

- **Análisis de Riesgo: “**Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo” (ISO/IEC 27000:2018).

- **Causa**: “Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo” (Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, Departamento Administrativo de la Función Pública, 2020).

- **Clase Riesgo Corrupción**: “Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado” (Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, Departamento Administrativo de la Función Pública, 2020).

- **Confidencialidad:** “Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados” (ISO/IEC 27000:2018).

- **Consecuencia:** “Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas” (Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, Departamento Administrativo de la Función Pública, 2020).

- **Contexto estratégico**: “Condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de la entidad” (Guía para la administración del riesgo, Cuarta Edición, Departamento Administrativo de la Función Pública, 2011).

- **Control:** “Medida por la que se modifica el riesgo” (ISO/IEC 27000:2018). “Las políticas, los procedimientos, las prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo” (Modelo de Seguridad y Privacidad de la Información, MinTIC, 2016).

- **Disponibilidad:** “Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada” (ISO/IEC 27000:2018).

- **Declaración de aplicabilidad:** "Documento que enumera los controles aplicados por el sistema de gestión de seguridad de la información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001" (ISO/IEC 27000:2018).

- **Evaluación del riesgo de Seguridad de la Información**: "Medición y evaluación continua de amenazas, impacto y vulnerabilidades sobre los activos de información, que permita la minimización de la ocurrencia de dichos riesgos. Proceso global de identificación, análisis y estimación de riesgos" (ISO/IEC 27000:2018).

- **Gestión de incidentes de seguridad de la información:** "Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información" (ISO/IEC 27000).

- **Impacto:** "En el contexto de la gestión de riesgos, corresponde a las consecuencias que puede ocasionar a la organización la materialización del riesgo" (Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, Departamento Administrativo de la Función Pública, 2020). "En el contexto de la gestión de incidentes, corresponde al costo para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc." (ISO/IEC 27000).

- **Integridad**: "La información debe ser precisa, coherente y completa desde su creación hasta su destrucción. Propiedad de la información relativa a su exactitud y completitud" (ISO/IEC 27000).

- **Probabilidad:** "Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad" (Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, Departamento Administrativo de la Función Pública, 2020).

- **Plan de tratamiento de riesgos:** "Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma" (ISO/IEC 27000:2018).

- **Privacidad:** "En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos

hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades públicas, la correlativa obligación de proteger dicha información en observancia del marco legal vigente" (Modelo de Seguridad y Privacidad de la Información, MinTIC, 2016).

- **Riesgo:** "Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales" (Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, Departamento Administrativo de la Función Pública, 2020)

- **Riesgo de seguridad de la información**: "potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización" (ISO/IEC 27000:2018).

- **Seguridad de la información:** "Preservación de la confidencialidad, integridad y disponibilidad de la información" (ISO/IEC 27000:2018).

- **Sistema de Gestión de Seguridad de la Información SGSI**: "Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua" (ISO/IEC 27000:2018).

- **Vulnerabilidad**: "Debilidad de un activo o control que puede ser explotada por una o más amenazas" (ISO/IEC 27000:2018).

3. OBJETIVO GENERAL

Identificar los riesgos de seguridad de la información de los procesos institucionales, permitiendo a los Líderes de cada proceso, mantener la confidencialidad, integridad y su disponibilidad de la información institucional.

4. OBJETIVOS ESPECÍFICOS

A. Realizar seguimiento a los riesgos de seguridad de la información asociados a los procesos tecnológicos existentes en el Ejército Nacional, haciendo su medición a través del Balanced Scorecard.

B. Fortalecer la aplicación de los controles de seguridad de la información para mitigar los riesgos de seguridad de la misma.

5. ALCANCE

La gestión de riesgos de seguridad de la información aplica a todos los servidores públicos (militares y civiles) del Ejército Nacional, Contratistas, Proveedores, Operadores y aquellas personas o terceros que, en razón del cumplimiento de los procesos y/o funciones compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los entes de control y entidades relacionadas que accedan, ya sea interna o externamente a cualquier archivo de información (bases de datos, plataforma tecnológica, software, drive, nube, entre otros), independientemente de su ubicación.

6. RECURSOS

A. Humano: Representantes institucionales, Líderes del Proceso (administración de infraestructura tecnológica, bases de datos, sistemas de información, gestión telemática, almacenamiento, disponibilidad, transmisión, entre otros), Profesionales en Tecnología, personal interno y personal externo.

B. Físico: Infraestructura tecnológica y equipos de comunicación.

C. Financiero: Planes de compras anuales institucionales.

D. Técnico: la metodología establecida en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, Departamento Administrativo de la Función Pública (DAFP), 2020.

7. RESPONSABLES DE LA GESTIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

- Líderes de Proceso.
- Oficiales de evaluación y seguimiento de cada proceso.

8. METODOLOGÍA DE IMPLEMENTACIÓN

Para llevar a cabo la identificación y tratamiento de los riesgos de seguridad y privacidad de la información, se seguirá la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP, autorizada por el Departamento de Planeación del Ejército Nacional (CEDE5), la Directiva Permanente N°000115 de 2019, “Lineamientos generales para la administración de Riesgos en el Ejército Nacional” y la Guía metodológica para la administración de riesgos 2022 del CEDE5.

De manera general, se señalan las siguientes actividades que se deben seguir en cada proceso, para la identificación y el tratamiento de los riesgos de seguridad de la información:

a. Identificación de los riesgos.
b. Análisis y valoración del riesgo.
c. Tratamiento de riesgos.
d. Monitoreo y revisión.
e. Comunicación y consulta.

De conformidad a lo anterior, la descripción detallada de las actividades se presenta en la Directiva Permanente N°000115 del 03 de diciembre 2019 “Lineamientos generales para la administración de riesgos en el Ejército Nacional”, en su anexo A “Metodología administración del riesgo”, y establece que la construcción de la matriz estratégica de riesgos y administración de riesgos se realiza teniendo como base la las causas establecidas en el formato “Contexto estratégico de administración de riesgos” código: FO-CEDE5-DIGEC-486. El contexto debe identificarse mediante la realización de mesas de trabajo con los Líderes de Procesos y Gestores de Calidad de cada uno de los procesos del Sistema Integrado de Gestión, definiendo factores internos y externos con sus causas. Posteriormente se realiza la consolidación, revisión y elaboración de un solo contexto estratégico de administración de riesgos para el Ejército Nacional, el cual será aprobado y publicado por el Departamento de Planeación, con el fin de estandarizar conceptos y con el cual deberán trabajar todos los procesos en la identificación de riesgos.

Conforme con lo anterior, para realizar la identificación de los riesgos de seguridad de la información, es necesario conocer primero su concepto, el cual, conforme a la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, del Departamento Administrativo de la Función Pública (DAFP), es:

> "Riesgo de seguridad de la información: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000)"[1].

Para la definición de los controles, los Líderes de Proceso deben analizar los siguientes procedimientos de seguridad de la información, para determinar cuáles son necesarios para reducir los riesgos, y que sirvan como guía para determinar los responsables, la periodicidad, propósito y evidencias del control.

1) Procedimiento de gestión de activos
2) Procedimiento de control de acceso
3) Procedimiento de acceso áreas seguras
4) Procedimiento de gestión de incidentes
5) Procedimiento de recolección de evidencia digital
6) Procedimiento de criptografía
7) Procedimiento de transferencia de información
8) Procedimiento de seguridad en sistemas de información
9) Procedimiento de medios removibles
10) Procedimiento de derechos de propiedad intelectual
11) Procedimiento de evaluación del SGSI
12) Procedimiento de gestión de cambios de infraestructura tecnológica
13) Procedimiento de registro de bases de datos con datos personales ante la Superintendencia de Industria y Comercio
14) Procedimiento de anonimización de datos personales estructurados

[1] COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la administración del riesgo y el diseño de controles en Entidades Públicas, Riesgos de Gestión, Corrupción y Seguridad Digital. (noviembre, 2020) Bogotá, D.C. Versión 5, p. 12. 2020.

15) Procedimiento de gestión de copias de respaldo

Los procedimientos se encuentran disponibles para su consulta en el portal web institucional y en la intranet.

Posteriormente, a la definición de los controles, es necesario valorar su efectividad e identificar el riesgo residual.

a. Tratamiento de riesgos

Para realizar el tratamiento de los riesgos residuales se debe seleccionar una opción de manejo, suministrando diversas tareas o actividades que puedan tener controlado el riesgo.

Teniendo en cuenta, que lo anterior es un proceso cíclico, se debe tratar el riesgo mediante un planeamiento, que debe identificar si los niveles de riesgo residual son tolerables, para luego asignar tareas y proceder a medirlas con indicadores de gestión en este aspecto.

Las estrategias que se pueden usar para tratar el riesgo son:

- Evitar el riesgo: se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- Reducir el riesgo: se adoptan medidas para reducir la probabilidad y/o el impacto del riesgo; por lo general conlleva a la implementación de controles.

- Compartir o transferir el riesgo: reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad.

- Asumir un riesgo: no se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

Después de determinar el tipo de estrategia para el tratamiento del riesgo, se deben establecer las acciones que se van a tomar para mitigar el riesgo. Estas acciones deben ser medibles y orientarse en un horizonte definido en el tiempo. De igual manera, deben ser actividades diferentes a las establecidas en la caracterización del proceso, procedimiento y reglamentación interna (reglamentos, normas, directivas permanentes, entre otras).

Adicionalmente, se deben establecer las acciones a ejecutar en caso de la materialización del riesgo, razón por la cual deben documentarse en un plan de mejoramiento (FO-CEIGE-165), antes de iniciar la vigencia. Esto servirá como plan de contingencia que se enmarcará dentro del Plan de Continuidad del Negocio y se considerará un control correctivo.

b. Monitoreo y revisión

Después de que las acciones para administrar los riesgos de seguridad de la información identificados en cada proceso sean diseñadas y validadas, es necesario establecer las actividades o estrategias para monitorearlos, teniendo en cuenta que estos nunca dejan de representar una amenaza para la integridad, disponibilidad y confidencialidad de la información institucional.

En consecuencia, el monitoreo es esencial para que cada proceso pueda asegurar que las acciones ejecutadas se estén llevando a cabo y así poder evaluar la eficacia de su implementación, realizando revisiones sobre la marcha para evitar situaciones que influyan en la aplicación de las acciones y en el avance de los indicadores.

El monitoreo de la administración de riesgos debe estar a cargo, en primera instancia, de los responsables de los procesos y en segunda instancia lo realizará las secciones de evaluación y seguimiento.

c. Comunicación y consulta

En esta fase se establece la comunicación con las partes internas y externas que intervienen durante los pasos de la metodología de administración de riesgos, con el fin de que estos sean consultados sobre su capacidad para cumplir con las acciones establecidas para el tratamiento de los riesgos de seguridad de la información identificados. De esta manera las partes involucradas son notificadas de sus responsabilidades frente a la gestión de los riesgos, y de los compromisos que deben cumplir en los tiempos establecidos, así como de los soportes de que se deben generar para evidenciar el cumplimiento de las acciones asignadas.

Por último, es necesario que los responsables de la gestión de riesgos de seguridad de la información en cada proceso, continúen trabajando en la revisión, aprobación e implementación de controles de seguridad de la información, orientados a reducir los riesgos de seguridad de la información.

9. CRONOGRAMA

Tabla 1. *Cronograma- Seguimiento e identificación riesgos seguridad de la información.*

ACTIVIDAD	ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Difusión plan de tratamiento de riesgos de seguridad de la información																								
Boletines de tratamiento de riesgos de seguridad de la información y normatividad aplicable																								

ACTIVIDAD	JULIO				AGOSTO				SEPTIEMBRE				OCTUBRE				NOVIEMBRE				DICIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Definición del contexto estratégico e Identificación de los riesgos.																								
Análisis y valoración del riesgo																								
Evaluación de controles																								
Definición del plan de tratamiento de riesgos																								
Aprobación de riesgos																								
Socialización de acciones para el tratamiento de los riesgos.																								

Fuente: *Dirección de Planeación y Políticas C5*

Nota: *Los Líderes y Oficiales de Evaluación y Seguimiento de cada proceso son responsables del cumplimiento de las actividades establecidas.*

10. SEGUIMIENTO Y EVALUACIÓN

Con la finalidad de valorar el impacto del plan y del funcionamiento de la gestión de riesgos, se determina evaluar los siguientes indicadores:

Tabla 2. *Indicador eficacia acciones del plan*

Nombre del indicador: eficacia acciones de control riesgos	
Meta: *Verificar el 100 % de cumplimiento de actividades de control establecidas para la gestión de los riesgos de seguridad de la información identificados para la vigencia 2023.*	
Meta año anterior: *N/A*	**Meta:***100 %*
Tipo de indicador: *Eficiencia (EFCC)*	**Formula del indicador:** *(V1/V2) x100*
Variable 1 – V1: *Total de actividades ejecutadas para la gestión de los riesgos de seguridad de la información vigencia 2023.* Fuente de información: las actividades a cumplir corresponden a las definidas en el formato FO-CEDE5-DIGEC-487, para los riesgos de	**Variable 2 – V2:** *Número de actividades de control establecidas en cada uno de los riesgos de seguridad de la información 2023.* Es la planeación de las actividades propuestas para la gestión de los riesgos de seguridad de la información de la vigencia 2023.

seguridad de la información vigencia 2023 y se monitorean por medio de la Suite Visión Empresarial.	
Evaluación: *trimestral*	**Tendencia:** *estable*

Fuente: *Dirección de Planeación y Políticas C5*

11. ENTREGABLES

- Actas de reunión como soporte de la gestión de riesgos de seguridad de la información del año 2023.
- Boletines de acuerdo a la programación con temas de seguridad de la información del año 2023.
- Matriz de riesgos del año 2024.

Firma,

Brigadier General **RUDDY ARIAS RODRÍGUEZ**
Jefe de Estado Mayor de Planeación y Políticas

Autentica,

Coronel **GIOVANNI ALBERTO GOMEZ RODRÍGUEZ**
Jefe del Departamento de Comunicaciones

Elaboró: PD0. Deicy Díaz
Servicios Tecnológicos
Gobierno Digital y Seguridad Digital

Revisó: ASJ. Yizel Quijano
Asesora Jurídica CEDE6

Vo.Bo.: TC. Andrés Zambrano
Director de Planeación y Políticas C5

Elaboró: Ti. David Arevalo
Oficial Diseño y Arquitectura C5

Revisó: PS. Laura Sandoval
Asesora Jurídica JEMPP

12. NORMATIVIDAD DE REFERENCIA

1) Ley 594 del 14 de julio de 2000, “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.

2) Decreto 2609 del 14 de diciembre de 2012, “Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado”.

3) Decreto 1078 del 26 de mayo de 2015, “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”.

4) Decreto 1008 del 14 de junio de 2018, “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

5) Resolución N° 0413 del 01 de marzo de 2021, “Por la cual se define el uso de las Tecnologías en la Nube para el Sector Defensa y se dictan otras disposiciones”.

6) Resolución N° 0004 del 26 de febrero de 2016, “Por la cual se reestructura el Ejército Nacional, se aprueban sus Tablas de Organización y Equipo TOE y se dictan otras disposiciones”.

7) Resolución N° 007722 del 25 de octubre de 2021, “Por la cual se crea el Comité Institucional de Gestión y Desempeño, el Modelo Integrado de Planeación y Gestión, el Modelo Estándar de Control Interno, el Subcomité Central de Coordinación del Sistema de Control Interno en el Ejército Nacional de Colombia, se dictan otras disposiciones y se deroga la resolución N°002420 de 2018 del 25 de octubre de 2018”.

8) Manual Operativo Sistema de Gestión, Modelo Integrado de Planeación y Gestión (MIPG), versión 2 de 2018.

9) Directiva Permanente N° 18 del 19 de junio de 2014, Ministerio de

Defensa Nacional, “Políticas de seguridad de la información para el sector defensa”.

10) Directiva Permanente N° 00196 del 27 de diciembre de 2017, Ejército Nacional, “Destrucción y disposición final de residuos de aparatos eléctricos electrónicos (RAEE)”, la que la modifique, aclare o adicione.

11) Directiva Permanente N° 00115 del 03 de diciembre de 2019, Ejército Nacional, “Lineamientos generales para la administración de riesgos en el Ejército Nacional”, la que la modifique, aclare o adicione.

12) Documento CONPES 3701 del 14 de julio de 2011, “Lineamientos de Política para Ciberseguridad y Ciberdefensa”.

13) Documento CONPES 3854 del 11 de abril de 2016, “Política Nacional de Seguridad Digital”.

14) Documento CONPES 3995 del 1 de julio de 2020, “Política Nacional de Confianza y Seguridad Digital”.

15) Guía metodológica para la administración de riesgos 2022 del Departamento de Planeación CEDE5.

13. BIBLIOGRAFÍA

Departamento Administrativo de la Función Pública. (2020). *Guía para la administración del riesgo y el diseño de controles en Entidades Públicas.* Bogotá: DAFP.

International Organization for Standardization. (2018). *ISO-IEC 27000 Tecnologías de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y vocabulario.* Suiza: ISO. Obtenido de: https://www.iso.org/standard/73906.html

Ministerio de Tecnologías de la Información y las Comunicaciones. (29 de Julio de 2016). *Modelo de Seguridad y Privacidad de la Información.* Obtenido de: https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf