Política Corporativa De Ciberresiliencia

Aprobado por el Consejo de Administración de El Corte Inglés, S.A. el 29 de octubre de 2025

Versión 1.0 de 29 de octubre de 2025

ÍNDICE

NOTA: En el **Anexo I** se relacionan las definiciones de aquellos términos que se utilizan de manera frecuente en el presente documento y en las normas relacionadas que conforman el Sistema de Gestión de Ciberresiliencia así como las que conforman el Sistema de Gestión de Compliance Penal de EL CORTE INGLÉS.

1. INTRODUCCIÓN

El Consejo de Administración de El Corte Inglés, S.A. tiene atribuida la responsabilidad de formular la Estrategia y las Políticas Corporativas de las empresas de El Grupo El Corte Inglés (en adelante, "El Grupo"), así como de aprobar los programas y sistemas de cumplimiento y control interno.

Desde sus orígenes, se ha considerado que la capacidad operativa en El Grupo constituye uno de sus activos estratégicos y es fundamental para la sostenibilidad y competitividad de la Organización. Es por ello que, con el objetivo de establecer los principios generales que deben regir la resiliencia cibernética en todas las empresas de El Grupo, el Consejo de Administración ha aprobado la siguiente Política Corporativa de Ciberresiliencia (en adelante, la "Política").

La presente Política está alineada con los valores de El Grupo, ratificando la firme voluntad de contribuir a los 17 Objetivos de Desarrollo Sostenible de Naciones Unidas y mantener una conducta respetuosa tanto con las normas exigibles a sus actividades, como con los estándares éticos y demás normas e iniciativas que el Grupo se compromete a respetar mediante su certificación o adhesión, tales como DORA, CRA, ENS, NIS2, etc. y las buenas prácticas como ISO/IEC 27001:2020, UNE-ISO/IEC 22301:2020, UNE-ISO/IEC 22316:2020 entre otras.

La Política constituye la base del Sistema de Gestión de Ciberresiliencia (en adelante, "SGCr"), a partir del cual se establecen la estrategia y operativa de la Organización.

2. OBJETIVO

El objetivo de esta Política es establecer los principios, compromisos y directrices que permite a El Grupo anticiparse, resistir, responder y recuperarse frente a amenazas y oportunidades, con afectación al ámbito cibernético, que puedan afectar la continuidad operativa, la seguridad e integridad de la información y la resiliencia organizacional.

La aplicación de dichos principios permite:

- reducir el impacto de los incidentes, con afectación al ámbito cibernético,
- el incremento de la capacidad de anticiparse y responder,
- la mejora continua del sistema de gestión y resiliencia organizacional,
- la continuidad operativa y mantener la confianza de los clientes,
- cumplir con la legislación vigente.

Esta Política busca ser un instrumento que promueva una toma de decisiones informada, alineada con el apetito de riesgo de El Grupo, los requerimientos regulatorios y las expectativas de las partes interesadas.

3. ÁMBITO DE APLICACIÓN

La presente Política es de obligado cumplimiento y de aplicación global a las sociedades que conforman El Grupo, empleados, colaboradores y terceros, en todas las actividades relacionadas

con la cadena de valor, tanto ascendente como descendente, independientemente del país en el que se desarrollen.

Todos los miembros de la Organización y socios de negocio, especialmente los trabajadores de la cadena de valor deberán cumplir con su contenido, independientemente del cargo que ocupen y del territorio desde donde operen.

Este compromiso debe formalizarse según se establece en el apartado "10. Conocimiento y declaración de conformidad" de la presente Política.

Asimismo, la Política se aplica en lo relativo a todos los recursos* en los distintos entornos operativos de El Grupo.

4. PRINCIPIOS DE ACTUACIÓN

El Grupo espera de cualquier miembro de la Organización, así como de sus socios de negocio y demás implicados el seguimiento de los siguientes principios de actuación, que sientan las bases con relación a la Ciberresiliencia Corporativa:

Principio 1. Gobernanza y liderazgo comprometido.

La Alta Dirección asume un papel activo en el desarrollo, supervisión y mejora de la ciberresiliencia, garantizando que se integren los objetivos de continuidad y resiliencia en la estrategia empresarial. Se deben asignar los recursos necesarios y se debe definir una gobernanza clara con roles y responsabilidades para la toma de decisiones, especialmente durante situaciones de crisis, con afectación al ámbito cibernético.

Principio 2. Cultura organizacional resiliente.

Se promueve una cultura organizacional orientada a la prevención, colaboración y respuesta proactiva frente a amenazas, con afectación al ámbito cibernético. Todo el personal debe recibir formación, concienciación y los mecanismos necesarios para actuar de manera coherente con los objetivos de resiliencia y seguridad.

Principio 3. Enfoque basado en la gestión de riesgos.

La estrategia de El Grupo se basa en la identificación y evaluación de los riesgos que puedan afectar sus procesos críticos, buscando una resiliencia cibernética efectiva. Esta evaluación se realiza de forma sistemática y continua, considerando amenazas internas y externas, para prevenir, priorizar acciones y garantizar la continuidad del negocio ante escenarios disruptivos.

Principio 4. Preparación y capacidad de respuesta.

La Organización desarrolla e implementa planes que garantizan una respuesta ágil y coordinada que limite el impacto de cualquier evento, con afectación al ámbito cibernético, sobre las operaciones y procesos críticos. Estos planes se deben probar anteriormente para asegurar que los involucrados saben cómo actuar de manera efectiva.

Principio 5. Protección de recursos críticos.

*Definición dentro del Anexo I

Se implementan controles y medidas de seguridad diferenciados para proteger los recursos más valiosos de la organización, incluyendo sistemas, datos, personas, procesos críticos, etc. La protección se basa en su nivel de criticidad y el impacto que una amenaza podría tener sobre la operación.

Principio 6. Comunicación eficaz.

El Grupo garantiza canales claros, accesibles y redundantes de comunicación interna y externa para el manejo de crisis, con afectación al ámbito cibernético. La información relevante fluye en tiempo real entre las partes interesadas, facilitando una respuesta eficiente, coherente y alineada con los principios de transparencia y responsabilidad.

Principio 7. Colaboración con terceros.

El Grupo traslada estos principios a los proveedores y las partes interesadas como parte de la gestión de los riesgos que afecten a los procesos críticos.

En consecuencia, en la contratación de proveedores, se debe asegurar que se trasladan tanto a nivel contractual como de formación los requisitos que emanen de la normativa interna en relación con proveedores.

Principio 8. Cumplimiento normativo y contractual.

La ciberresiliencia se gestiona en conformidad con las leyes, regulaciones, estándares y compromisos contractuales aplicables en materia de seguridad de la información, resiliencia y continuidad del negocio. Se audita periódicamente el cumplimiento y se gestionan los cambios normativos de manera proactiva.

Principio 9. Transparencia y mejora continua.

Se establece un ciclo de revisión y mejora que incorpora lecciones aprendidas, resultados de simulacros, auditorías internas y cambios en el entorno tecnológico. La Política, los controles y los procedimientos de ciberresiliencia se actualizan de forma sistemática para asegurar su efectividad a lo largo del tiempo.

Estos principios constituyen la base operativa y estratégica sobre la cual se construye la capacidad de la Organización para resistir, adaptarse y recuperarse de amenazas cibernéticas, asegurando su sostenibilidad y competitividad a largo plazo.

5. ESTRUCTURA ORGANIZATIVA

El SGCr del Grupo establece una estructura organizativa basada en tres pilares fundamentales: el Gobierno, la Gestión y la Operación de la Ciberresiliencia.

5.1. Gobierno de la Ciberresiliencia

El Gobierno se asienta en la **Dirección de Prevención y Seguridad Corporativa**, órgano rector encargado de liderar, coordinar y supervisar la estrategia global de seguridad y ciberresiliencia, garantizando su alineación con los objetivos corporativos y la normativa aplicable.

Bajo su supervisión se estructuran los siguientes órganos colegiados:

- **Gabinete Asesor en materia de Crisis, Emergencias y Catástrofes:** órgano principal y de mayor relevancia, de carácter consultivo y de apoyo estratégico a la Alta Dirección, encargado de asesorar en la toma de decisiones críticas, recomendar la activación de planes de gestión de crisis y coordinar la interlocución con autoridades y organismos externos.

*Definición dentro del Anexo I

- **CSI (Comité de Seguridad de la Información):** comité multidisciplinar y periódico que impulsa y supervisa la seguridad de la información en toda la organización, asegurando que las buenas prácticas se apliquen de manera transversal y consistente.

5.2. Gestión de la Ciberresiliencia

La **Gestión** se articula a través del **Área de Ciberresiliencia**, integrada en el marco de GRC. Esta unidad coordina, define y regula las capacidades de ciberresiliencia del Grupo, asegurando la coherencia de las actuaciones en todos los ámbitos organizativos y promoviendo la adopción de política, procedimientos y controles comunes.

5.3. Operación de la Ciberresiliencia

La **Operación** recae en las **áreas operativas** responsables de ejecutar las medidas y capacidades de ciberresiliencia. Estas áreas aseguran la correcta aplicación de los recursos requeridos para mantener la resiliencia organizativa, incluyendo: personas, ubicaciones, tecnología, terceros, seguridad, etc.

6. COMPONENTES DEL SGCr

El Sistema de Gestión de Ciberresiliencia (SGCr) es el marco organizativo adoptado por El Grupo, con cuatro componentes fundamentales sobre los que se articula su eficaz funcionamiento:

- **Estrategia de Ciberresiliencia:** aproximación de alto nivel definida por el Grupo con el objetivo de tener la capacidad de anticiparse, resistir y recuperarse frente a las amenazas. Incluye documentos que presentan la declaración de los principios y valores de la organización sobre la ciberresiliencia y su alineación con la estrategia corporativa y los objetivos de negocio.
- **Marco Normativo de Ciberresiliencia:** desarrollo de un conjunto de Políticas, Normas, Procedimientos generales y específicos que abarcan los requisitos identificados tanto en el Marco de Control, como en las regulaciones aplicables.
- **Marco de Control de Ciberresiliencia:** Establece la estructura técnica y organizativa de controles para adaptar, proteger activos, gestionar riesgos y asegurar la recuperación de los procesos de negocio de El Grupo.
- **Cuadro de Mando de Ciberresiliencia:** herramienta que permite medir y evaluar el desempeño de las acciones y procesos relacionados.

Estos cuatro componentes son mantenidos y actualizados según el contexto y las necesidades de la Organización por el Departamento de Seguridad de Información y Ciberseguridad.

7. ANÁLISIS LEGAL Y REGULATORIO

El Grupo reconoce la necesidad de cumplir con todas las obligaciones legales, reglamentarias y contractuales relacionadas con la seguridad de la información, la privacidad de los datos y la continuidad del negocio. En ese sentido, el componente legal de la ciberresiliencia es considerado una prioridad estratégica.

Marco normativo aplicable

La organización se compromete a identificar y cumplir con la legislación vigente en todas las jurisdicciones donde opera, incluyendo, pero no limitado a:

- **Leyes de protección de datos personales**, como el Reglamento General de Protección de Datos (GDPR) en Europa.

*Definición dentro del Anexo I

- **Normativas de ciberseguridad específicas** para el sector retail o para industrias reguladas (por ejemplo, PCI-DSS para manejo de tarjetas, ISO, ENS, etc.).
- **Leyes de notificación obligatoria de incidentes**, como aquellas que exigen informar sobre brechas de datos a autoridades o afectados.
- **Requisitos de supervisores financieros o de consumo**, cuando apliquen a plataformas de pago, comercio electrónico o servicios de crédito.

Obligaciones contractuales

Se incluye el análisis de cláusulas de seguridad y resiliencia en los contratos con terceros, socios tecnológicos, operadores logísticos y proveedores de servicios en la nube, garantizando que:

- se especifique la responsabilidad en caso de incidentes de seguridad,
- se definan tiempos máximos de respuesta y notificación (SLA) y
- se incluya el derecho de auditoría en relación con controles de seguridad

8. NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

La identificación y gestión de las necesidades y expectativas de las partes interesadas es fundamental para asegurar que estén alineadas con el contexto interno y externo de El Grupo.

Las siguientes partes interesadas han sido identificadas como clave para el desempeño, la sostenibilidad y la resiliencia de la organización:

PARTE INTERESADA	ROL
Clientes	Usuarios finales de productos y servicios.
Empleados	Ejecutores de procesos, operadores de sistemas y atención al cliente.
Responsable del proceso de negocio	Marcan los requisitos mínimos para asegurar que los procesos críticos pueden llevarse a cabo.
Alta dirección y accionistas	Responsables del gobierno corporativo y estrategia de negocio.
Proveedores y terceros	Suministro de productos, tecnología y servicios críticos.
Entidades regulatorias	Supervisión del cumplimiento legal y normativo.
Socios comerciales	Alianzas estratégicas, franquiciados y operadores logísticos.
Comunidad y sociedad	Entorno social, ambiental y económico.
Organismos de respuesta	Cuerpos de seguridad, autoridades de protección civil y CERTs.

De acuerdo con los principios de las normas ISO 22301 e ISO 22316, comprender las necesidades y expectativas de las partes interesadas es esencial para fortalecer la continuidad operativa y la resiliencia organizacional. Esta identificación permite alinear las capacidades de respuesta con los requisitos del entorno y generar confianza entre los actores clave. A continuación, se presentan las principales necesidades y expectativas según el rol de cada parte interesada:

*Definición dentro del Anexo I

Clientes

- Acceso ininterrumpido a canales de venta (físicos y digitales).
- Protección de sus datos personales y financieros.
- Transparencia en caso de incidentes que los afecten.
- Confianza en la disponibilidad y seguridad de los servicios.

Empleados

- Capacitación sobre roles y responsabilidades en ciberresiliencia y continuidad.
- Canales seguros de trabajo, especialmente en esquemas híbridos o remotos.
- Procedimientos claros ante incidentes o crisis.
- Confianza en la organización como lugar seguro y estable para trabajar.

Responsable del proceso de negocio

- Definición y validación de los requisitos de continuidad de negocio y tiempos de recuperación (RTO/RPO) aplicables a sus procesos.
- Aseguramiento de la disponibilidad de recursos clave (tecnología, personal, instalaciones) en escenarios de interrupción.
- Información oportuna sobre riesgos y vulnerabilidades que puedan afectar sus operaciones.
- Participación en ejercicios de simulación, pruebas y revisiones del sistema de gestión de la continuidad y ciberresiliencia.
- Coordinación fluida con TI, seguridad de la información y gestión de crisis para alinear las capacidades de respuesta con los objetivos del negocio.
- Toma de decisiones informada basada en datos de impacto al negocio (BIA) y análisis de riesgos.
- Confianza en que la organización protege y prioriza la resiliencia de los procesos críticos para la continuidad operativa.

Alta dirección y accionistas

- Alineación de la ciberresiliencia con la estrategia empresarial.
- Minimización del impacto financiero, operativo y reputacional ante crisis.
- Cumplimiento normativo y reducción de riesgos legales.
- Reportes claros sobre el estado de preparación organizacional.

Proveedores y terceros

- Estándares claros de seguridad y continuidad exigidos en contratos.
- Definición de SLA y tiempos de recuperación (RTO/RPO).
- Procedimientos de comunicación ante incidentes.
- Interoperabilidad y confianza mutua en situaciones de contingencia.

Entidades regulatorias y de cumplimiento

- Cumplimiento de leyes de protección de datos (ej. GDPR).
- Notificación oportuna y adecuada ante brechas de seguridad.
- Disponibilidad de evidencia documental sobre planes, pruebas y controles.
- Participación en auditorías o inspecciones si es requerido.

Socios comerciales y franquiciados

- Aseguramiento de la continuidad de operaciones compartidas.

*Definición dentro del Anexo I

- Integridad de los datos transaccionales.
- Acceso a plataformas corporativas con altos estándares de seguridad.
- Apoyo y alineación ante incidentes mayores o crisis reputacionales.

Comunidad y sociedad

- Comportamiento ético y responsable de la organización.
- Gestión de crisis que minimice el impacto en consumidores y empleo.
- Transparencia en la comunicación pública de eventos graves.
- Contribución a la estabilidad social y económica del entorno.

Organismos de respuesta ante emergencias

- Coordinación efectiva en caso de desastres o ataques cibernéticos.
- Acceso a información clave sobre incidentes.
- Colaboración en simulacros o ejercicios conjuntos.

Estas necesidades y expectativas se revisan periódicamente mediante análisis del contexto organizacional, encuestas y reuniones con partes clave.

Se utilizan herramientas como el mapeo de influencia e impacto, así como el monitorización de quejas y no conformidades. Esto garantiza una adaptación continua a los cambios del entorno y refuerza la resiliencia de El Grupo.

9. DILIGENCIA DEBIDA

Los procesos de diligencia debida hacen referencia a la gestión y monitorización de la relación con terceros, bien sean estos proveedores, clientes, socios comerciales o cualquier otra tercera parte con la que medie relación contractual y den, o potencialmente puedan dar, soporte a los procesos de negocio de la Organización.

El proceso de diligencia debida con terceros se asienta bajo los siguientes pilares:

- Antes de establecer una relación con una tercera parte, se debe evaluar el impacto del acuerdo en la Ciberresiliencia y, si hay impacto, realizar el análisis de riesgos correspondiente.
- La Organización debe establecer un marco de controles y medidas que permita de forma normalizada y sistemática gestionar los riesgos de seguridad vinculados a la colaboración o contratación de terceras partes.
- La tercera parte se debe comprometer contractualmente al cumplimiento de la Política de Ciberresiliencia y a la implantación de las medidas técnicas y organizativas que aseguren la correcta protección de los recursos de la Organización.
- De forma periódica y en base el nivel de riesgo asociado al acuerdo, se deben llevar a cabo procesos de monitorización y auditoría que aseguren que la tercera parte mantiene un ecosistema de seguridad equivalente al comprometido contractualmente.
- A la finalización de la relación contractual, la Organización debe asegurar la devolución de los recursos, la destrucción de la información y la revocación de accesos a la información por parte del tercero.

*Definición dentro del Anexo I

10. CONOCIMIENTO Y DECLARACIÓN DE CONFORMIDAD

El cumplimiento de las normas y estándares éticos compromete a toda la Organización y constituye un objetivo estratégico para la misma, por ello, se espera que todos los Miembros de la Organización conozcan y respeten el contenido de esta Política. Igualmente, y respecto de Socios de Negocio, se espera que desarrollen comportamientos alineados con la misma.

Este compromiso debe formalizarse mediante:

i. Declaraciones de conformidad con los principios en ellas desarrollados por parte de los Miembros de la Organización, a través de su adhesión a los **Altos Estándares Éticos**,

ii. **Cláusulas en materia de Cumplimiento incluidas en los contratos** con Socios de Negocio

iii. **Adhesiones expresas o tomas de razón** por parte de los órganos de Administración de las empresas que forman parte de El Grupo Corte Inglés, según normativa interna elaborada al respecto.

Estas adhesiones y sus renovaciones deberán comunicarse, cuando se formalicen, a la Dirección de Cumplimiento y Control de Riesgos de El Grupo El Corte Inglés.

Cuando se produzcan cambios significativos en esta Política, entendiendo por éstos los que requieran una aprobación formal por parte del Consejo de Administración de El Corte Inglés, S.A. deberán renovarse formalmente los compromisos anteriores.

Puesto que el cumplimiento de las normas y estándares éticos compromete a toda la Organización y constituye un objetivo estratégico para la misma, se espera que todos los Miembros de la Organización conozcan y respeten el contenido de esta Política. Igualmente, y respecto de Socios de Negocio, se espera que desarrollen comportamientos alineados con la misma.

La Organización reaccionará de forma inmediata ante eventuales incumplimientos de lo establecido en esta Política, conforme a lo previsto en su normativa interna y de acuerdo con la legislación vigente que resulte de aplicación.

11. COMUNICACIÓN DE INCUMPLIMIENTOS

11.1 Incumplimientos de la normativa de seguridad de la información

Todos los Miembros de la Organización, Socio de Negocio o Tercero con relación directa e interés comercial o profesional legítimo, y demás partes interesadas, en caso de detectar un incumplimiento de la presente Política o de tener dudas sobre si alguna práctica observada puede suponer un acto ilícito, ya sea en el sector público como en el privado, está obligado a ponerse inmediatamente en contacto con la Dirección de Cumplimiento y Control de Riesgos del Grupo El Corte Inglés a través del Canal Ético, en cualquiera de sus vías de comunicación:

- **Canal Digital:**

  El Grupo El Corte Inglés dispone de un canal digital al que se puede acceder a través de la siguiente dirección web:

  https://www.elcorteingles.es/informacioncorporativa/es/gobierno-corporativo/etica-y-cumplimiento/

  Este acceso está disponible en la web corporativa y adicionalmente en la intranet NEXO para los Miembros de la Organización

*Definición dentro del Anexo I

- **Dirección postal:**

  El Corte Inglés, S.A.
  Dirección de Cumplimiento y Control de Riesgos
  c/ Hermosilla, 112
  28009 Madrid

- **Teléfono Departamento Cumplimiento Normativo:** 91 401 85 00

- **Solicitud de reunión presencial o por medios telemáticos**

La información transmitida por este Canal es confidencial, así como la identidad de los informantes, a los que la Organización agradece su colaboración y respecto a los cuales garantiza la ausencia de represalias.

Además, la Dirección de Cumplimiento y Control de Riesgos podrá actuar por propia iniciativa investigando cualquier indicio de incumplimiento de esta Política.

12. APROBACIÓN, ENTRADA EN VIGOR Y ACTUALIZACIÓN

La presente Política entra en vigor en la fecha de aprobación por el Consejo de Administración de El Corte Inglés, S.A.

Esta Política debe mantenerse actualizada en el tiempo. Para ello, debe revisarse de forma ordinaria con periodicidad anual y, de forma extraordinaria, y en todo caso, a la mayor brevedad, cuando se produzcan variaciones significativas en los objetivos estratégicos o en la normativa externa o interna aplicable que implique su actualización o modificación.

Las propuestas de modificación se deben presentar a la Comisión de Auditoría y Control por parte del Comité de Seguridad de la Información, previa validación de la Dirección de Asesoría Jurídica y de la Dirección de Cumplimiento y Control de Riesgos y con la correspondiente supervisión del órgano de control interno que tenga atribuida la función.

En caso de que los cambios sean relevantes, deberán someterse a la aprobación del Consejo de Administración previa propuesta de la Comisión de Auditoría y Control.

13. DIFUSIÓN Y APLICACIÓN

La presente Política estará disponible en NEXO para todos los Miembros de la Organización y en la web corporativa para todos los grupos de interés del Grupo, una vez sea aprobada por el Consejo de Administración de El Corte Inglés, S.A.

Asimismo, el Comité de Seguridad de la Información se ocupará de impulsar las acciones necesarias para su adecuada difusión y conocimiento.

14. CONTROL, SEGUIMIENTO Y SUPERVISIÓN

14.1 Control y seguimiento

El Subcomité de Ciberresiliencia evaluará periódicamente el cumplimiento y la eficacia de esta Política mediante revisiones, controles y auditorías internas y externas coordinados por el Departamento de Seguridad de Información y Ciberseguridad, e informará del resultado al Comité de Seguridad de la Información.

*Definición dentro del Anexo I

Corresponde al Comité de Seguridad de la Información la supervisión de forma continua de la aplicación de lo dispuesto en esta Política por parte de las empresas del Grupo.

14.2 Supervisión

El departamento de Auditoría Interna revisará la adecuación y la eficacia de las medidas aplicadas en el SGCr para supervisar el cumplimiento de las normativas aplicables a las distintas actividades de la Organización en la medida en que el Plan Anual de Auditoría aprobado por la Comisión de Auditoría y Control incluya trabajos vinculados con dicho Sistema, y extraordinariamente, como consecuencia de la ocurrencia de incidencias o identificación de irregularidades. Como resultado de dichas auditorías, Auditoría Interna debe emitir el correspondiente informe, emitiéndose recomendaciones en caso de identificarse oportunidades de mejora.

Las oportunidades de mejora que potencialmente puedan identificarse como resultado de estas revisiones, deben considerarse en el proceso de mejora continua del Sistema.

La valoración de un posible incumplimiento de la Política Corporativa de Ciberresiliencia se debe determinar en el procedimiento correspondiente, según las disposiciones vigentes, sin perjuicio de las responsabilidades legales, incluso de carácter sancionador en el ámbito laboral, que, en su caso, puedan resultar exigibles al incumplidor.

*Definición dentro del Anexo I

CONTROL DE CAMBIOS

Versión 1.0 aprobada por el Consejo de Administración el 29 de octubre de 2025

Versión	Fecha Modificación	Objeto de la Modificación	Apartados afectados
		-	-

Última revisión, 29 de octubre 2025

*Definición dentro del Anexo I

Anexos

Anexo I - Definiciones

Se relacionan a continuación las definiciones de aquellos términos que se utilizan de manera frecuente en el presente documento.

Activo de información: es cualquier recurso, componente o elemento de valor para una Organización que debe ser protegido, gestionado y, en su caso, recuperado para asegurar la continuidad y seguridad de las operaciones.

Amenaza: circunstancia desfavorable que puede ocurrir y que cuando sucede tiene consecuencias negativas sobre los activos o recursos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor.

Ciberresliencia o resiliencia cibernética: capacidad de una Organización para anticipar, resistir, responder y recuperarse de eventos adversos, garantizando la continuidad de sus operaciones y la protección de sus activos y recursos críticos frente a amenazas, con afectación al ámbito cibernético.

Confidencialidad: se refiere a la protección de datos y sistemas para evitar amenazas como el acceso no autorizado o la fuga de datos que podría resultar en la divulgación, alteración o destrucción de información sensible.

Crisis: es cualquier evento, incidente o conjunto de circunstancias que interrumpe gravemente la disponibilidad o integridad de los procesos de negocio, con afectación al ámbito cibernético, afectando de forma significativa la capacidad de la organización para operar con normalidad y que requiere una respuesta inmediata y coordinada para mitigar daños, restaurar funciones críticas y proteger los recursos.

Disponibilidad: capacidad de un servicio, un sistema o proceso, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran.

Efectivo: que produce el efecto esperado. Se refiere al resultado logrado, sin importar los medios, el tiempo o los recursos utilizados.

Eficaz: que logra el objetivo deseado. Se centra en alcanzar el resultado, pero sin entrar en si fue costoso o se usaron muchos recursos.

Eficiente: que logra un objetivo utilizando la menor cantidad de recursos posibles (tiempo, dinero, esfuerzo...).

Evento: es cualquier ocurrencia identificable dentro de un sistema, red o entorno tecnológico que puede tener relevancia para la seguridad de la información o el funcionamiento normal de los procesos. Un evento no implica necesariamente una amenaza o daño, pero puede ser un indicio de un posible incidente o actividad anómala.

Incidente de seguridad: cualquier suceso que afecte a la confidencialidad, integridad o disponibilidad de los activos de información de la Organización, por ejemplo: acceso o intento de acceso a los sistemas, uso, divulgación, modificación o destrucción no autorizada de información.

Integridad: propiedad de la información, por la que se garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración o pérdida.

Política de Seguridad de la Información: documento de nivel ejecutivo mediante el cual la Organización establece sus directrices, decisiones y medidas de seguridad respecto a la seguridad

*Definición dentro del Anexo I

de sus sistemas de información después de evaluar el valor de sus activos y los riesgos a los que están expuestos.

Resiliencia: capacidad de una organización para construir, asegurar y revisar su integridad y fiabilidad operativas para sustentar la prestación continuada de los servicios.

Recurso: todos los activos (incluyendo infraestructura y equipos), personas, habilidades, tecnología, locales, suministros e información que la Organización deben tener a su disposición para utilizar cuando sea necesario con el fin de operar y cumplir su objetivo.

Riesgo: es la posibilidad de que se produzcan incidentes o eventos que comprometan la confidencialidad, integridad o disponibilidad de los datos y sistemas de la Organización.

Seguridad de la Información: conjunto de tecnologías, prácticas y medidas diseñadas para proteger la confidencialidad, integridad y disponibilidad de la información.

Sistema de Gestión: conjunto de elementos de una organización interrelacionados que interactúan para establecer políticas, objetivos y procesos.

*Definición dentro del Anexo I