Política de roles y responsabilidades

Telefonica IoT & Big Data Tech SA

Política

Sistema Integrado de Gestión

N05-POL-Política de roles y responsabilidades-SIG-PUB

v 5.0

Índice

Hoja de Control

Titulo	Política de roles y responsabilidades		
Código	N05-POL-Política de roles y responsabilidades-SIG-PUB		
Autor	Planificación y estrategia (SIG) o Área responsable		
Clasificación	Público	**Tipo documento**	Procedimiento
Revisado por	Responsable SIG	**Fecha revisión**	08/09/2022
Aprobado por	Comité SIG	**Fecha aprobación**	29/09/2022

Control de Cambios

Versión	Fecha	Autore	Descripción
1.0	25/03/2022	SIG	Versión Inicial
2.0	27/04/2022	SIG	Clasificación Pública.
2.1	31/05/2022	SIG	Corrección del hallazgo 2022_AE_ENS&27001_Fase Doc_NC-02.
2.2	03/08/2022	SIG	Añadida la información específica del “Comité de gestión del SIG” para de Calidad y Medioambiente.
3.0	09/09/2022	SIG	Versión aprobada.
3.1	19/09/2022	SIG	Corrección hallazgo 2022_AI_9001&14001_OB-06
4.0	29/09/2022	SIG	Versión aprobada.
4.1	30/09/2022	SIG	Descripción de las responsabilidades del apartado 3.4.1.
4.2	20/02/2023	SIG	Revisada auditoria ISO 2700
5.0	14/04/2023	SIG	Versión aprobada.

1. Objetivo

La presente política tiene por objetivo definir y designar los roles, responsabilidades y autoridades que tengan relación directa con los procesos estratégicos del Sistema Integrado de Gestión (en adelante SIG) implantado en IoT & BD.

2. Alcance

Todos los aspectos relacionados con el objetivo del presente documento que se encuentran recogidos bajo el alcance definido para el SIG de IoT & BD.

3. Política

3.1. Procedimiento de designación y renovación de roles

La creación del Comité de gestión del SIG (Comité del SIG), el nombramiento de sus integrantes y la designación de los responsables identificados en esta Política, se revisará al menos anualmente en la revisión por Dirección SIG para la renovación del rol o cuando la persona cambie su puesto de trabajo o cuando el puesto quede vacante.

La relación entre las personas y los roles aquí definidos quedará vigente mediante un acta.

3.2. Dirección General

Sus funciones principales en relación con el SIG son la dirección estratégica y garantizar la provisión de recursos.

3.3. Comités

Los comités de gestión tienen la función de dirigir y coordinar el Sistema Integrado de Gestión, procurando la eficacia y eficiencia de los procesos que lo constituyen y asegurando su adecuación a lo dispuesto por las normas Implantadas en el SIG.

3.3.1. Comité de gestión del SIG

El Comité del SIG es el órgano constituido por personas con la capacidad de gestionar la calidad, el medioambiente y la seguridad de la información en la organización, es designado por la Dirección General y tiene asignadas las siguientes funciones dentro de la organización:

- Responsabilizarse de la Gestión del Sistema Integrado de Seguridad, Calidad y Medioambiente.
- Definición de nuevas medidas para mejorar la seguridad la calidad y medioambiente.

- Revisión de la Política, normas, procedimientos y documentación relacionada con seguridad de la información, calidad y medioambiente.

Se reunirá tantas veces como lo designen sus integrantes, pero por lo menos se deberá reunir una vez al año de manera ordinaria para realizar la Revisión por Dirección. En caso de que el Comité lo considere oportuno y debido a circunstancias que así lo requieran, se podrán convocar reuniones extraordinarias.

A las reuniones del Comité del SIG puede invitar, de manera excepcional, a aquellas personas que el éste considere oportunas según los temas a tratar.

Se redactará un acta de cada reunión del Comité del SIG. Las reuniones de este Comité pueden hacerse coincidir con las del Comité de Revisión por la Dirección. Las reuniones de Comité se dan por finalizadas formalmente, cuando todos los integrantes aprueban el contenido del Acta. Estas actas se archivan por el responsable del SIG, o por otra persona en la que se delegue esta tarea, en formato digital.

3.3.2. Subcomité local de seguridad

Este Comité se constituye con el objetivo de alinear la estrategia de seguridad del grupo con la de la organización.

- Coordinar los esfuerzos de las diferentes áreas en materia de Seguridad de la Información, para asegurar que sean consistentes, alineados con la estrategia decidida en la materia, y evitar duplicidades.

- Resolver los conflictos de responsabilidad en materia de seguridad que puedan surgir entre los diferentes roles.

3.4. Roles generales

3.4.1. Responsable del SIG

El Responsable del SIG cumple la función de supervisar técnicamente el correcto seguimiento de las necesidades de las partes interesas para cumplir con la Calidad, Medioambiente así como la Seguridad de la Información de la Organización y se responsabiliza de:

- Asegurarse de que los sistemas de gestión son conforme con los requisitos de esta Norma de referencia Internacional.

- Asegurarse de que los procesos están generando y proporcionando las salidas previstas.

- Informar, en particular, a la alta dirección sobre el desempeño de los sistemas de gestión, y sobre las oportunidades de mejora.

- Asegurarse de que se promueve el enfoque al cliente en toda la organización.
- Asegurarse de que la integridad del sistema de gestión se mantiene cuando se planifican e implementan cambios en el sistema de gestión.
- Asegurarse de analizar el impacto en los aspectos ambientales cuando se planifican e implementan cambios en el sistema de medioambiente.
- Conocer los requerimientos de cliente.
- Seguimiento de la satisfacción de los clientes.
- Recoger las quejas de los clientes.
- Coordinar los procesos del SIG.
- Elaborar informes.
- Informar a los proveedores de la evaluación interna correspondiente.
- Asesorar en materia de Seguridad de la Información, Calidad y Medioambiente, a los integrantes de la Organización.
- Implementar, coordinar y controlar, en toda la organización, las medidas de seguridad definidas en la documentación del SIG, mediante la efectiva implementación de los controles.
- Identificar las tendencias y cambios significativos en los riesgos de Calidad, Medioambiente y Seguridad de la Información y, en su caso, coordinado con los responsables o propietarios de los Riesgos, consensuar modificaciones de los controles con él.
- Seguimiento y revisión de las incidencias de seguridad acontecidas. Revisar la información registrada de los controles.
- Elaborar informes de las revisiones efectuadas.
- Supervisar la monitorización del estado de seguridad del sistema.
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.
- Asegurar que los objetivos de seguridad han sido claramente identificados, están alineados con los requerimientos de la Organización y quedan integrados en los procesos críticos, aportando contenido en materia de seguridad a los procesos de negocio.

- Revisar las Políticas de Calidad, Medioambiente y Seguridad de la Información y la efectividad de su implementación y cumplimiento, en coordinación con los Comités del SIG y Seguridad de la Información.

- Adoptar las medidas necesarias para que el personal conozca las normas en materia de seguridad que afectan al desarrollo de sus funciones y de las consecuencias en que pudieran incurrir en caso de incumplimiento.

- Análisis de los informes de las auditorías de seguridad de la información. Elevar a la Dirección General las conclusiones de los informes de auditoría.

3.4.2. Responsable de Seguridad

El responsable de la Seguridad se responsabiliza de gestionar la seguridad lógica y física que da soporte al sistema de la gestión de la información.

Es quien debe coordinar los planes basados en metodologías, de tal forma que garanticen la seguridad de la información en sus tres dimensiones (Disponibilidad, Integridad y Confidencialidad).

Debe tener conocimientos de la norma ISO/IEC 27001:2013 y nociones técnicas relacionados con la seguridad dentro del alcance, dado que se apoyará en el responsable de calidad y seguridad.

Tiene asignadas las siguientes funciones dentro de la organización:

- Actualizar la documentación del SIG, siempre que sea necesario.

- Mantener informado al personal sobre las acciones llevadas a cabo y la implementación de nuevas funcionalidades, así como recomendar las mejores prácticas en materia de Seguridad de la Información.

- Definición/revisión de normas y procedimientos de seguridad, en colaboración con el Responsable de Calidad y Seguridad de la Información.

- Proponer las medidas necesarias para mantener la seguridad según el estado de las nuevas tecnologías intentando avanzarse a las posibles consecuencias de una brecha de seguridad.

- Análisis de los informes de las auditorías de calidad y seguridad de la información.

3.4.3. Responsable de Sistemas

El responsable de Sistemas, según lo determina el Esquema Nacional de Seguridad (ENS), asumiendo al menos las siguientes funciones:

- Desarrollar, operar y mantener el Sistema de Información durante todo su ciclo de vida, según sus especificaciones, incluyendo su instalación y la verificación de su correcto funcionamiento, apoyándose en el personal, interno o externo, que se considere necesario.

- 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, en coordinación con el Responsable de la Seguridad.

- El Responsable del Sistema puede acordar la suspensión del manejo de una cierta información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos, previa consulta con el Responsable de la Seguridad y el Responsable del Servicio, antes de ser ejecutada.

3.4.4. Responsable de la Información

Al responsable de la Información se le atribuyen las siguientes funciones:

- Establecer y aprobar los requisitos de seguridad aplicables a la información dentro del marco establecido en el anexo I de Real Decreto 3/2010, de 8 de enero, previa propuesta del responsable de seguridad y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten a la Información.

3.4.5. Responsable del Servicio

Al responsable del servicio se le atribuyen las siguientes funciones:

- Establecer y aprobar los requisitos de seguridad aplicables el servicio dentro del marco establecido en el anexo I de Real Decreto 3/2010, de 8 de enero, previa propuesta del responsable de seguridad y/o Comité de Seguridad de la Información.
- Aceptar los niveles de riesgo residual que afecten al Servicio.

3.4.6. Responsable de People

El Responsable de People lo es de todo lo relacionado con la gestión del personal de la organización. Dentro de las tareas que realiza se definen las siguientes:

- Supervisa la incorporación de Personal, previa aprobación por Dirección. Posteriormente el candidato es evaluado por el responsable del área a la que corresponde la petición.
- Gestiona las formaciones y capacitaciones del personal.
- Evalúa y gestiona el desempeño de los diferentes perfiles de la empresa.
- Distribuye las políticas y normativa de IoT & BD a todos los empleados.

3.4.7. Auditores

Las personas designadas en el plan para realizar las auditorías internas de seguridad de la información pueden ser:

- Personal de la Organización, calificado como auditor.
- Auditores externos cualificados.

En todo caso, los auditores no tendrán relación directa con las actividades o áreas a auditar.

El personal de la Organización que actúe como auditor deberá estar debidamente cualificado para ello, exigiéndose los siguientes requisitos:

- Poseer conocimientos mínimos sobre sistemas de gestión.
- Poseer conocimientos sobre las normas ISO y el ENS.
- Haber realizado al menos una auditoria en prácticas.

3.4.8. Responsable de seguridad DPO (Protección de datos)

El Responsable de Seguridad o DPO (Protección de Datos) es el rol encargado de velar por el cumplimiento de las medidas de seguridad que dispone el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas física. Puede compartir el cargo con en el Responsable del SIG o el de Seguridad.

3.4.9. Propietario del riesgo

Es el rol que tiene asignada la responsabilidad de gestionar determinado riesgo, es decir, con autoridad para tomar decisiones sobre el tratamiento de ciertos riesgos de seguridad de la información.

Tiene asignadas las siguientes funciones dentro de la organización:

- Aprobar el Plan de tratamiento de riesgos para los riesgos de los que es propietario, en coordinación con la Dirección.

- Aprobar los riesgos residuales, resultantes del tratamiento de riesgos, para los riesgos de los que es propietario, en coordinación con la Dirección.

Puede compartir el cargo con en el Responsable del SIG o el de Seguridad.

3.4.10. Responsable de Legal

El rol de Responsable de Legal consiste en verificar que el funcionamiento de los servicios es acorde a los requisitos legales y compromisos contractuales adquiridos por la organización.

4. Documentación relacionada

- Normativa del Grupo Telefónica

5. Anexos

5.1. Requisitos mínimos de seguridad (Artículo 11 del ENS)

Mediante la presente política de roles y responsabilidades, se completan los requisitos mínimos ENS, complementarios a la política Global de Seguridad de corporativo.

De este modo, se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.

IoT&BD. ha organizado su seguridad comprometiendo a todos los miembros de la organización designando diferentes roles de seguridad con responsabilidades claramente diferenciadas, como se indica en la sección "ORGANIZACIÓN DE SEGURIDAD" de este documento.

b) Análisis y gestión de los riesgos.

Todos los sistemas afectados por esta Política de Seguridad, así como todo el procesamiento de datos personales, deben estar sujetos a un análisis de riesgos, evaluando las amenazas y riesgos a los que están expuestos. Este análisis se repetirá:

Regularmente, al menos una vez al año.

Cuando la información manejada y/o los servicios proporcionados cambian significativamente.

Cuando se produce un incidente de seguridad grave o se detectan vulnerabilidades graves.

El jefe de seguridad ENS será el encargado de llevar a cabo el análisis de riesgos, así como de identificar deficiencias y debilidades e informarles del Comité de Seguridad de la Información.

c) Gestión de personal & d) Profesionalidad.

Todos los miembros de IoT&BD, dentro del ámbito de la ENS, asistirán a una sesión mínima de concienciación sobre la seguridad una vez al año. Se establecerá un programa de sensibilización continua para atender a todos los miembros, en particular a los recién incorporados.

Las personas responsables del uso, funcionamiento o administración de los sistemas TIC recibirán capacitación para la gestión segura de los sistemas en la medida en que lo necesiten. La formación será obligatoria antes de asumir una responsabilidad, ya sea su primera asignación o si se trata de un cambio de trabajo o responsabilidades en ella.

e) Autorización y control de los accesos.

IoT&BD ha implementado mecanismos de control del acceso al sistema de información, limitándose a aquellos estrictamente necesarios y debidamente autorizados.

f) Protección de las instalaciones.

IoT&BD ha implementado mecanismos de control de acceso físico, evitando el acceso físico no autorizado, así como daños a la información y los recursos, a través de perímetros de seguridad, controles físicos y protecciones generales en diferentes áreas.

g) Adquisición de productos.

Para la adquisición de productos, IoT&BD, tendrá en cuenta que estos productos han certificado la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en los que los requisitos de proporcionalidad con respecto a los riesgos asumidos no lo justifiquen, a juicio del Responsable de Seguridad.

h) Seguridad por defecto.

IoT&BD diseña y configura los sistemas de forma que garanticen la seguridad por defecto, incluyendo lo siguiente:

- El sistema proporcionará la mínima funcionalidad requerida para que la organización alcance sus objetivos.

- Las funciones de operación, administración y registro de actividad serán las mínimas necesarias, y se asegurará que sólo son accesibles por las personas, o desde emplazamientos o equipos, autorizados, pudiendo exigirse en su caso restricciones de horario y puntos de acceso facultados.

- En un sistema de explotación se eliminarán o desactivarán, mediante el control de la configuración, las funciones que no sean de interés sean innecesarias e, incluso, aquellas que sean inadecuadas al fin que se persigue.

- El uso ordinario del sistema ha de ser sencillo y seguro, de forma que una utilización insegura requiera de un acto consciente por parte del usuario.

i) Integridad y actualización del sistema.

IoT&BD ha implementado controles y evaluaciones de seguridad regulares (incluidas las evaluaciones de los cambios de configuración de forma rutinaria), para conocer en todo momento el estado de seguridad de los sistemas en relación con las especificaciones de los fabricantes, vulnerabilidades y actualizaciones que les afectan, reaccionando diligentemente para gestionar el riesgo en vista de su estado de seguridad. Antes de la entrada de nuevos elementos, ya sean físicos o lógicos, estos requerirán un análisis formal.

Asimismo, solicitará la revisión periódica por parte de terceros para obtener una evaluación independiente.

j) Protección de la información almacenada y en tránsito.

IoT&BD, ha implementado mecanismos para proteger la información almacenada o en tránsito, especialmente cuando se encuentra en entornos inseguros (portátiles, móviles, tabletas, medios de información, redes abiertas, etc.).

Los sistemas dispondrán de copias de seguridad y establecerán los mecanismos necesarios para garantizar la continuidad de las operaciones en caso de pérdida de los medios de trabajo habituales.

Se han desarrollado procedimientos que garantizan la recuperación y conservación a largo plazo de documentos electrónicos producidos en el ámbito de las competencias de IoT&BD. Del mismo modo, se han implementado mecanismos de seguridad de conformidad con la naturaleza del soporte en el que se encuentran los documentos, para garantizar que toda la información relacionada con el soporte no electrónico esté protegida con el mismo grado de seguridad que la electrónica.

k) Prevención ante otros sistemas de información interconectados.

IoT&BD ha implementado una estrategia de protección basada en múltiples capas, consistente en medidas organizativas, físicas y lógicas, de modo que cuando una de las capas falla, el sistema implementado permite:

- Ahorre tiempo para una reacción adecuada a los incidentes que no han podido evitar.
- Reduzca la probabilidad de que el sistema se vea comprometido en su conjunto.
- Minimice el impacto final en él.

Esta estrategia debe proteger el perímetro, en particular, si se conecta a las redes públicas. En cualquier caso, se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

l) Registro de actividad.

IoT&BD ha habilitado registros de la actividad del usuario al retener la información necesaria para monitorear, analizar, investigar y documentar actividades inadecuadas o no autorizadas, permitiendo identificar en todo momento a la persona que actúa. Todo ello con el único fin de lograr el cumplimiento del objeto de este Real Decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar, a la imagen de los afectados, y de acuerdo con la normativa de protección de datos personales o laborales, y otras disposiciones aplicables.

m) Incidentes de seguridad.

IoT&BD ha implementado un proceso integral de detección, reacción y recuperación contra código dañino a través del desarrollo de procedimientos que cubren los mecanismos de detección, criterios de clasificación, procedimientos de análisis y resolución, así como canales de comunicación a las partes interesadas y el registro de acciones. Este registro se utilizará para la mejora continua de la seguridad del sistema.

Para que la información y/o los servicios no se ven perjudicados por incidentes de seguridad, IoT&BD, implementa las medidas de seguridad establecidas por la ENS, así como cualquier otro control adicional, que ha identificado como necesario, mediante una evaluación de amenazas y riesgos. Estos controles, así como las funciones y responsabilidades de seguridad de todo el personal, están claramente definidos y documentados.

Cuando haya una desviación significativa de los parámetros que han sido preestablecidos como normales, se establecerán los mecanismos de detección, análisis e informe necesarios para que lleguen a los responsables regularmente.

IoT&BD establecerá las siguientes medidas de reacción a los incidentes de seguridad:

- Mecanismos para responder eficazmente a los incidentes de seguridad.

- Designe un punto de contacto para las comunicaciones con respecto a los incidentes detectados en otros departamentos o en otras agencias.

- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambas direcciones, con los Equipos de Respuesta a Emergencias (CERT).

Para garantizar la disponibilidad de los servicios, IoT&BD, cuenta con los medios y técnicas necesarios que garantizan la recuperación de los servicios más críticos.

n) Continuidad de la actividad.

IoT&BD ha habilitado registros de la actividad del usuario al retener la información necesaria para monitorear, analizar, investigar y documentar actividades inadecuadas o no autorizadas, permitiendo identificar en todo momento a la persona que actúa. Todo ello con el único fin de lograr el cumplimiento del objeto de este Real Decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar, a la imagen de los afectados, y de acuerdo con la normativa de protección de datos personales o laborales, y otras disposiciones aplicables.

o) Mejora continua del proceso de seguridad.
IoT&BD promueve la mejora continua del sistema de gestión de la seguridad de la información. Para ello, será responsable de:

- Coordinar los esfuerzos de las diferentes áreas en el campo de la Seguridad de la Información, para asegurar que sean consistentes, alineadas con la estrategia decidida en la materia, y evitar duplicidades.

- Proponer planes para mejorar la seguridad de la información, con su correspondiente dotación presupuestaria, priorizando las acciones de seguridad cuando los recursos son limitados.

- Asegúrese de que la seguridad de la información se tiene en cuenta en todos los proyectos desde su especificación inicial hasta su lanzamiento. En particular, tendrá que garantizar la creación y el uso de servicios horizontales que reduzcan las duplicaciones y apoyen el funcionamiento homogéneo de todos los sistemas TIC.

- Supervisar los principales riesgos residuales asumidos por la Administración y recomendar posibles acciones con respecto a ellos.

- Supervise la gestión de incidentes de seguridad y recomiende posibles acciones con respecto a ellos.

- Preparar y revisar periódicamente la Política de Seguridad de la Información para su aprobación por el organismo competente.

- Elaborar procedimientos de seguridad de la información para su aprobación en caso de que sea necesario.
- Verifique los procedimientos de seguridad de la información y otra documentación para su aprobación.
- Desarrollar programas de formación destinados a la formación y sensibilización entre el personal de seguridad de la información y, en particular, en el ámbito de la protección de datos personales.
- Elaborar y aprobar los requisitos de formación y cualificación de administradores, operadores y usuarios desde el punto de vista de la Seguridad de la Información.

Promover el desempeño de auditorías periódicas ENS y protección de datos que permitan verificar el cumplimiento de las obligaciones de la Administración en materia de Seguridad de la Información.

Público

Telefónica Tech

tech.telefonica.com