POLÍTICA SEGURIDAD DE LA INFORMACIÓN

CONTENIDO

MISIÓN CORPORATIVA **4**

ALCANCE **4**

VISIÓN ESTRATÉGICA **4**

VALORES ESTRATÉGICOS 4

COMPROMISOS DE BC DIGITAL **5**

PRINCIPIOS GENERALES: 6

PRINCIPIOS PARTICULARES Y RESPONSABILIDADES ESPECÍFICAS 7

ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD **8**

ALCANCE DE LA POLÍTICA DE SEGURIDAD 8

SEGREGACIÓN DE TAREAS EN EL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 8

ASIGNACIÓN DE ROLES EN SEGURIDAD DE LA INFORMACIÓN 9

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 9

ANÁLISIS Y GESTIÓN DE RIESGOS **10**

GESTIÓN DEL PERSONAL **10**

PROFESIONALIDAD **11**

AUTORIZACIÓN Y CONTROL DE ACCESO **12**

PROTECCIÓN DE LAS INSTALACIONES **12**

ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD **12**

SEGURIDAD POR DEFECTO **12**

INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA **13**

PROTECCIÓN DE INFORMACIÓN ALMACENADA Y EN TRÁNSITO **13**

PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS 14

REGISTRO DE ACTIVIDAD.....14

INCIDENTES DE SEGURIDAD 14

CONTINUIDAD DE LA ACTIVIDAD.....14

MEJORA CONTINUA DEL PROCESO DE SEGURIDAD.....15

ANEXO I: LEGISLACIÓN APLICABLE.....16

MISIÓN CORPORATIVA

BC DIGITAL nace como empresa proveedora de servicios tecnológicos, desarrollando aplicaciones informáticas y participando en el outsourcing de personal dando respuestas eficaces de principio a fin a los problemas y retos con los que se enfrentan las organizaciones.

ALCANCE

El Sistema de Gestión de seguridad de la información llevado a cabo en el centro de Miguel Yuste 26, Madrid da soporte a los procesos de:

Desarrollo de Software de Gestión Empresarial y Explotación en Entornos Cloud según la Declaración de Aplicabilidad

(Management Software and Cloud Products Delivery under SOA).

VISIÓN ESTRATÉGICA

BC DIGITAL quiere llegar a ser una empresa que cumpla los siguientes criterios:

- *Ser una empresa eficaz a partir de criterios de calidad y satisfacción de cliente.*
- *Ser una empresa rentable y sostenible para sus accionistas.*
- *Ser una empresa de alta responsabilidad social con el medioambiente y las personas.*
- *Ser una empresa segura y confiable en materia de seguridad de la información para todas sus partes interesadas.*

VALORES ESTRATÉGICOS

BC DIGITAL declara que sus valores principales son:

- *Calidad de servicio.*

- *Respeto al entorno.*
- *Sostenibilidad y protección del medio ambiente*
- *Profesional*
- *Confianza.*
- *Seguridad*

COMPROMISOS DE BC DIGITAL

Para ello BC DIGITAL adquiere los siguientes compromisos:

En **general**:

- *Mejora continua del desempeño tanto de los sistemas de gestión como del resultado a obtener. Mejora de la eficacia de los sistemas.*
- *Actualización y cumplimiento del marco legal y de los requisitos propios y específicos que nos puedan poner tanto nuestros clientes como los proveedores y personas implicadas.*
- *Disponer de un sistema de gestión que garantice la protección del medio ambiente y seamos capaces de responder a las condiciones ambientales cambiantes, no sólo previniendo impactos ambientales adversos mediante la prevención de la contaminación si no también mediante el uso sostenible de los recursos, la mitigación y adaptación al Cambio Climático y la protección de la Biodiversidad y de los Ecosistemas en lo referido al alcance de nuestras actividades.*
- *Mantener un alto nivel de cualificación y talento para poder ser eficaces y eficientes en los procesos.*

- *Mantenimiento de los adecuados canales de comunicación con todas las partes interesadas, con objeto de asegurar su satisfacción con respecto al cumplimiento de sus necesidades, requisitos y expectativas*
- *Se adoptarán las medidas necesarias para que todo el personal de BC DIGITAL sea conocedor de esta política. Difundiéndose también ésta a los proveedores y colaboradores, estando además a disposición del público a través de la página web.*

En **seguridad de la información**:

PRINCIPIOS GENERALES:

- *Política de Análisis, gestión y Disminución del riesgo potencial grave. Se priorizarán las actuaciones sobre riesgos potenciales graves.*
- *Política de Tolerancia con las incidencias. Se investigará y sancionará aquellas actuaciones dolosas o imprudentes.*
- *Política de impacto reputacional mínimo. La incidencia reputacional en materia de seguridad debe tender a 0. Integridad y actualización de los sistemas*
- *La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema, evitando, salvo casos de urgencia o necesidad, cualquier actuación puntual o tratamiento coyuntural. La seguridad de la información debe considerarse como parte de la operativa habitual, estando presente y aplicándose desde el diseño inicial de los sistemas de información*
- *Controlar operacionalmente de forma eficaz las amenazas y riesgos sobre el activo y las instalaciones.*
- *Organizar el sistema por medio de la implementación de los procesos de seguridad que se revisan y mejoran de forma continua*
- *Política de Seguridad por defecto: Los sistemas deben diseñarse y configurarse de forma que garanticen un grado suficiente de seguridad por defecto.*

- *Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación vigente en materia de seguridad de la Información*

PRINCIPIOS PARTICULARES Y RESPONSABILIDADES ESPECÍFICAS

- *Gestionar eficientemente las incidencias que afecten a la integridad, disponibilidad y confidencialidad de la información de la empresa.*
- *Implantar planes de continuidad del negocio que garanticen la continuidad de las actividades de la sociedad en caso de incidencias graves o contingencias.*
- *Política de gestión de personas como activo de información que incluya medidas de sensibilización y/ o formación en materia de seguridad*
- *Gestionar los roles de los profesionales responsables del sistema de seguridad de la información para asegurar el nivel de profesionalidad necesario.*
- *Política de control y autorización de accesos se limitará el acceso a los activos de información por parte de usuarios, procesos y otros sistemas de información mediante la implantación de los mecanismos de identificación, autenticación y autorización acordes a la criticidad de cada activo.*
- *Política de seguridad física de las instalaciones Los activos de información serán emplazados en áreas seguras, protegidas por controles de acceso físicos adecuados a su nivel de criticidad. Los sistemas y los activos de información que contienen dichas áreas estarán suficientemente protegidos frente a amenazas físicas o ambientales.*
- *Política de criterios de seguridad de la información aplicados a la gestión de proveedores y en la Adquisición de productos (sistemas y servicios)*
- *Protección de datos (inactivos y en tránsito/medios) se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos.*
- *Prevención contra la conexión a través de sistemas interconectados*

- *Registro de actividad*
- *Protección de los sistemas y de la comunicación: se establecerán los procedimientos necesarios para lograr una adecuada gestión de la seguridad, operación y actualización de las Tecnologías de la Información y Comunicaciones. La información que se transmita a través de redes de comunicaciones deberá ser adecuadamente protegida, teniendo en cuenta su nivel de sensibilidad y de criticidad, mediante mecanismos que garanticen su seguridad.*
- *Política de gobernanza y gestión de la IA: lideraremos una adopción ética y segura de las tecnologías de Inteligencia Artificial (IA), garantizando que su despliegue no comprometa los pilares fundamentales de la seguridad de la información. La Dirección asegura que todo sistema de IA será gestionado bajo un marco de gobernanza estricto, diseñado para proteger la confidencialidad de los datos de entrenamiento y entrada, salvaguardar la integridad de los modelos y sus resultados frente a manipulaciones o sesgos, y asegurar la disponibilidad de los servicios críticos basados en esta tecnología*

ORGANIZACIÓN E IMPLANTACIÓN DEL PROCESO DE SEGURIDAD

ALCANCE DE LA POLÍTICA DE SEGURIDAD

El alcance de esta política afectará a todos los miembros de la organización y deberá ser conocida por todos ellos.

SEGREGACIÓN DE TAREAS EN EL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Para asegurar la segregación de tareas las siguientes funciones no se asignan a las mismas personas:

a) Operación de sistemas

b) Desarrollo

c) Auditoría de los sistemas de información

d) Directivo en Seguridad de la Información.

ASIGNACIÓN DE ROLES EN SEGURIDAD DE LA INFORMACIÓN

El personal en roles de confianza es designado por el Comité de Seguridad con la aprobación de la Dirección Ejecutiva y están libres de conflictos de intereses. Los roles de confianza incluyen:

- Director de Sistemas (CISO): Responsable de la operación de sistemas
- CTO: Responsable de los procesos de desarrollo y determinará los requisitos de los servicios prestados
- Responsable Sistema Integrado de Gestión: Responsable de la realización de Auditoria de los sistemas
- CSO: Directivo de seguridad de la información determinará las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios
- Director de Producción:Administrador del equipo: Privilegios sobre el equipo para realizar cambios sobre el usuario y sistema del equipo incluyendo la instalación de programas.

Así mismo en el procedimiento de gestión de roles y responsabilidades se asignan DERECHOS DE ACCESO A HERRAMIENTAS SEGÚN los siguientes roles:

- Dirección
- Jefe de Proyecto
- Desarrollador
- Analista / Negocio
- Servicios centrales (RRHH)
- Analista
- Sistemas/Operaciones

COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

El comité estará formado por:

- Director de sistemas
- CEO
- CTO
- CSO

- Responsable de sistema Integrado de gestión
- DPO

Se contará con asesores externos en materia de ciber seguridad y en función del riesgo a abordar y del tipo de medidas a tomar, así como de la integración de las medidas en el sistema de seguridad de la información.

Los responsables de líneas de negocio afectados participarán en las sesiones del comité de seguridad para ayudar con las responsabilidades de supervisión y personal de gestión de riesgos para escalar las discrepancias significativas en los análisis de riesgos de seguridad que les afecten.

ANÁLISIS Y GESTIÓN DE RIESGOS

BC DIGITAL cuenta con un procedimiento de gestión de riesgos de seguridad de la información basado en la metodología MAGERIT, reconocida internacionalmente. Contemplando las siguientes condiciones:

- Los riesgos se evalúan al menos anualmente por el comité de seguridad y los propietarios de activos.
- Se establece y revisa el apetito de riesgo anualmente por parte de la dirección
- Se definen planes de tratamiento de riesgos en función del apetito de riesgo establecido

GESTIÓN DEL PERSONAL

BC Digital ha establecido una política específica de seguridad de personas en la que se contempla la normas a aplicar en seguridad de la información así como necesidad de la formación anual en materia de seguridad de la información de todo el personal y de forma específica del personal directamente relacionado con el sistema de seguridad de la información.

Así mismo se cuenta con un plan de sensibilización anual que de forma continua mantiene informada a la plantilla de posibles campañas de ingeniería social, vulnerabilidades de aplicaciones, entre otras.

El personal relacionado con la información y los sistemas ejercitará y aplicará los principios de seguridad en el desempeño de su cometido:

- Seguridad integral. La seguridad se entenderá como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema
- Gestión de riesgos. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
- Prevención, reacción y recuperación. Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Las medidas de detección estarán acompañadas de medidas de reacción, de forma que los incidentes de seguridad se atajen a tiempo. Las medidas de recuperación permitirán la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.
- Líneas de defensa. El sistema ha de disponer de una estrategia de protección constituida por múltiples capas de seguridad
- Reevaluación periódica. Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección,
- Función diferenciada. En los sistemas de información se diferenciará el responsable de la información, el responsable del servicio y el responsable de la seguridad.

BC DIGITAL cuenta con una política de control de accesos donde se establece que cada usuario que acceda a la información del sistema debe estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado determinada actividad.

PROFESIONALIDAD

BC DIGITAL cuenta con un plan de auditorías internas y externas anual realizadas por personal cualificado conforme al perfil de auditor definido en el procedimiento de auditoría interna en materia de seguridad de la información en los referenciales:

UNE EN ISO 27001

Calificación PINAKES nivel A

Esquema Nacional de Seguridad Nivel Alto

AUTORIZACIÓN Y CONTROL DE ACCESO

Por medio del procedimiento de autorización y la política de control de accesos BC DIGITAL vela porque el acceso al sistema de información será controlado y limitado a los usuarios, procesos, dispositivos y otros sistemas de información, debidamente autorizados, restringiendo el acceso a las funciones permitidas.

PROTECCIÓN DE LAS INSTALACIONES

BC DIGITAL cuenta con una política de seguridad física, así como un procedimiento asociado donde se contemplan las medidas adoptadas en materia de seguridad física entra las que se encuentran:

- Control de acceso
- Control de llaves
- Identificación de zonas seguras

ADQUISICIÓN DE PRODUCTOS DE SEGURIDAD

BC DIGITAL dispone de un procedimiento de adquisición de productos de seguridad de las tecnologías de la información y comunicaciones que determina el criterio a cumplir en función del uso previsto del producto a que se refiera.

SEGURIDAD POR DEFECTO

El sistema de seguridad de la información de BC DIGITAL se diseña y configura para garantizar la seguridad por defecto:

a) El sistema proporcionará la mínima funcionalidad requerida para que la organización sólo alcance sus objetivos, y no alcance ninguna otra funcionalidad adicional.

b) 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.

c) 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.

d) 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.

INTEGRIDAD Y ACTUALIZACIÓN DEL SISTEMA

Para asegurar la integridad y actualización del sistema BC DIGITAL ha implantado los procedimientos de gestión y adquisición de activos, así como el de monitorización del sistema para asegurar que:

- Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.
- Se conoce en todo momento el estado de seguridad de los sistemas, en relación con las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de estos.

PROTECCIÓN DE INFORMACIÓN ALMACENADA Y EN TRÁNSITO

BC DIGITAL se compromete con la protección de la información por medio de:

- la clasificación de la información y la asignación de medidas específicas de seguridad que se recogen en el procedimiento de gestión documental.
- La protección de la información en tránsito por medio de la política de gestión de activos y de dispositivos móviles en los que se establecen las medidas de los dispositivos en tránsito.
- El procedimiento de seguridad operacional en el que se contemplan las medidas de recuperación electrónica de la información y los sistemas de copia de seguridad.

PREVENCIÓN ANTE OTROS SISTEMAS DE INFORMACIÓN INTERCONECTADOS

Desde BC DIGITAL se analizarán los riesgos derivados de la interconexión del sistema, a través de redes, con otros sistemas, y se controlará su punto de unión.

REGISTRO DE ACTIVIDAD

Con la finalidad exclusiva de lograr el cumplimiento del objeto RD 3/2010 con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, y demás disposiciones que resulten de aplicación, se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

INCIDENTES DE SEGURIDAD

Por medio del procedimiento de gestión de incidentes de seguridad BC DIGITAL establece un sistema de:

- Detección y reacción frente a código dañino.
- Registro de los incidentes de seguridad que se produzcan y las acciones de tratamiento que se sigan.
- Estos registros se emplearán para la mejora continua de la seguridad del sistema

CONTINUIDAD DE LA ACTIVIDAD

Por medio de los procedimientos de continuidad de negocio y gestión de continuidad de negocio, así como el de gestión de crisis se establecen los mecanismos para asegurar la continuidad de las operaciones en caso de pérdida de los medios habituales de trabajo.

MEJORA CONTINUA DEL PROCESO DE SEGURIDAD

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua.

Y como compromiso con el cumplimiento de esta política firma la Dirección.

Director General
BC Digital

ANEXO I: LEGISLACIÓN APLICABLE

La legislación aplicable se controla mediante la herramienta Wordlex,