POLÍTICA SEGURIDAD DE LA INFORMACIÓN

ESTADO DE REVISIÓN/MODIFICACIÓN DEL DOCUMENTO

N.º EDICIÓN	Fecha	Naturaleza de la Revisión
00	03/04/2017	Edición inicial
01	03/01/2019	Inclusión de la SSI
02	15/10/2020	Adecuación BC DIGITAL
03	17/05/2021	Mejora de la política de seguridad
04	21/12/2021	Incluir referencia explícita a la protección del medio ambiente
05	15/02/2022	Separación de Política de seguridad de la política de gestión integrada e incorporación de requisitos ENS
06	08/03/2022	Incorporación ENS
07	02/06/2022	Incorporación de estructura de documentación del sistema
08	20/09/2022	Declaración de Aplicabilidad versión 6

ELABORADO	REVISADO	APROBADO
RESPONSABLE DE SIG	CSO	DIRECCIÓN
Firmado: Laura Gómez	Firmado: Javier Vicente	Firmado: Domingo Almaraz

CONTENIDO

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 v3

(Management Software and Cloud Products Delivery under SOA v6).

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*

- *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.*

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 27001:2013

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.

ESTRUCTURACIÓN DE LA DOCUMENTACIÓN DE SEGURIDAD DEL SISTEMA, SU GESTIÓN Y ACCESO

La estructuración de la documentación de seguridad del sistema se gestiona por medio del procedimiento de información documentada y contempla los siguientes niveles, criterios de clasificación y accesos autorizados.

Nivel	Criterios de clasificación	Accesos
Confidencial	Información que contiene credenciales de acceso a los sistemas informáticos o a la información de BC DIGITAL Análisis de riesgos o documentación que aporte información sobre debilidades presentes en la organización. (contraseñas, secretos y cualquier información sensible en este apartado)	Alta dirección Personal Técnico con responsabilidades acordes (Sistemas, Financiero) autorizados por Alta Dirección

Restringida	Documentación que contiene información relativa a la infraestructura informática. Documentación que contiene información funcional de las aplicaciones de software desarrolladas Código fuente aplicaciones desarrolladas BCDIGITAL	Alta dirección Personal Técnico con responsabilidades acordes (Sistemas, Responsables de Desarrollo)
Interna	Procedimientos de gestión de la organización	Todo el personal BC Digital
Pública	El resto de documentación.	

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 a 2 de junio de 2022

Domingo Almaraz
CIO
BC Digital

ANEXO I: LEGISLACIÓN APLICABLE

NORMATIVA DE SEGURIDAD NACIONAL
Ley de Seguridad Nacional
Consejo Nacional de Ciberseguridad
Mecanismos para garantizar funcionamiento integrado Sistema de Seguridad Nacional
Estrategia de Seguridad Nacional
Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
Reglamento de Evaluación y Certificación de Seguridad de Tecnologías de la Información
Comité de Seguridad de los Sistemas de Información de la Seguridad Social
Comité de Seguridad de las Tecnologías de la Información
Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica
Real Decreto-ley de seguridad de las redes y sistemas de información
Ley reguladora del Centro Nacional de Inteligencia
Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia
Ley sobre secretos oficiales

Desarrollo de las disposiciones de la Ley sobre Secretos Oficiales

Ley Orgánica de los estados de alarma, excepción y sitio

Ley de Secretos Empresariales

Estrategia Nacional de Ciberseguridad 2019

INFRAESTRUCTURAS CRÍTICAS

Ley que establece medidas para la protección de las infraestructuras críticas

Reglamento de protección de las infraestructuras críticas

Contenidos de Planes de Seguridad del Operador y de Planes de Protección Específicos

NORMATIVA DE SEGURIDAD

Servicios Centrales y Periféricos de la Dirección General de la Policía (parcial)

Ley Orgánica de protección de la seguridad ciudadana

Ley de Seguridad Privada

Reglamento de Seguridad Privada

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD

Ley de servicios de la sociedad de la información y de comercio electrónico (parcial)

Centro Criptológico Nacional

Organización básica de las Fuerzas Armadas (parcial)

Desarrollo de la organización básica del Estado Mayor de la Defensa (parcial)

TELECOMUNICACIONES Y USUARIOS

Ley de servicios de la sociedad de la información y de comercio electrónico

Medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos

Distintivo público de confianza en los servicios de la sociedad de la información

Ley de acceso electrónico de los ciudadanos a los Servicios Públicos

Desarrollo parcial de la Ley de acceso electrónico de los ciudadanos a los servicios públicos

Ley reguladora de determinados aspectos de los servicios electrónicos de confianza

Expedición del documento nacional de identidad y sus certificados de firma electrónica

Ley General de Telecomunicaciones

Reglamento sobre el uso del dominio público radioeléctrico

Protección del dominio público radioeléctrico

Ley de conservación de datos relativos a comunicaciones electrónicas y redes públicas

Formato de entrega datos conservados por los operadores

CIBERDELINCUENCIA

Ley Orgánica del Código Penal (parcial)

Ley Orgánica reguladora de la responsabilidad penal de los menores (parcial)

Ley de Enjuiciamiento Criminal (parcial)

PROTECCIÓN DE DATOS

Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales

Reglamento de la Ley Orgánica de protección de datos de carácter personal

Reglamento Europeo relativo a protección en el tratamiento de datos personales

RELACIONES CON LA ADMINISTRACIÓN

LOPD (Ley Orgánica de Protección de Datos) [2] y el nuevo reglamento europeo de protección de datos RGPD [16], para proteger la vida privada de las personas y sus datos en las comunicaciones electrónicas;

LSSI-CE (Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico) [3] que regula los aspectos jurídicos de las actividades económicas o lucrativas del comercio electrónico, la contratación en línea, la información y la publicidad y los servicios de intermediación;

LPI (Ley de Propiedad Intelectual) [4], que regula los derechos relativos a las creaciones literarias, artísticas o científicas, en formatos tradicionales (fotografía, pintura, literatura,…) y en formatos digitales (imágenes, videos, contenido multimedia, libros digitales …), incluido el software;

Leyes de Propiedad Industrial [5], que protegen diseños industriales, marcas y nombres comerciales, patentes y modelos de utilidad;

Reglamento europeo de identificación electrónica y servicios de confianza en el mercado interior [6], para reforzar la confianza en las transacciones electrónicas entre ciudadanos, empresas y las AAPP en el marco del Mercado Único Digital Europeo.

Ley 11/2007 de acceso electrónico de los ciudadanos a los servicios públicos

Real Decreto 3/2010, Esquema Nacional de Seguridad

Decisión 2001/844/CE CECA, Euratom de la Comisión, de 29 de noviembre de 2001 por la que se modifica su Reglamento interno y Decisión 2001/264/CE del Consejo

Normativa nacional sobre Procedimiento Administrativo Ley 30/1992.

Normativa nacional sobre Administración Electrónica Ley 11/2007.

Protección de Datos de Carácter Personal Ley Orgánica 15/1999.

Firma Electrónica y DNI electrónico Ley 59/2003.

Centro Criptológico Nacional.

Reutilización de la información en el sector público Ley 37/2007.

Directrices y Guías de la OCDE.

Disposiciones nacionales e internacionales sobre normalización.

ANEXO I. REFERENCIAS DEL ESQUEMA NACIONAL DE SEGURIDAD

- Guía NIST SP 800-100. An introduction to Computer Security: The NIST Handbook. October, 1995.

- Guía CCN-STIC 201. Organización y Gestión para la Seguridad de las TIC.

- Guía CCN-STIC 301. Requisitos STIC.

- Guía CCN-STIC 400. Manual de Seguridad de las Tecnologías de la Información y Comunicaciones.

- Guía CCN-STIC 402. Organización y Gestión para la Seguridad de los Sistemas TIC.

- Guía CCN-STIC 803. Valoración de los Sistemas.

- Guía CCN-STIC 804. ENS-Guía de Implantación.

- Guía CCN-STIC 814. Seguridad en correo electrónico.

- Guía CCN-STIC 815. Métricas e indicadores en el ENS.

- FIPS 200. Minimum Security Requirements for Federal Information and Information Systems.

- Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

- Real Decreto 1671/2009, de 6 de septiembre, de desarrollo parcial de la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.

- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

- Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad del en ámbito de la administración electrónica.

- Guía NIST SP 800-53. Recommended Security Controls for Federal Information Systems and Organizations.

- Guía NIST SP 800-100. Information Security Handbook: A Guide for Managers.

- UNE - ISO/IEC 27002:2005 Código de buenas prácticas para la Gestión de la Seguridad de la información.

- UNE - ISO/IEC 27001:2007 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información

NORMATIVA DE SEGURIDAD DE BC DIGITAL

20210525_BCD_NORM_POLT_ESP_ARQ_SEG_V1.docx
20210525_BCD_NORM_POLT_ESP_ARQ_SEG_ZT.docx
20200917_BCD_NORM_POLT_ESP_CONTRASEÑAS.docx
20210525_BCD_NORM_POLT_ESP_CIFR_INF.docx
20200917_BCD_NORM_POLT_ESP_CONT_NEG.docx
20200917_BCD_NORM_POLT_ESP_GEST_ACT.docx
20200917_BCD_NORM_POLT_ESP_HW_DISP_MOV_ALMAC
20210207_BCD_NORM_POLT_ESP_MONIT.docx
20210525_BCD_NORM_POLT_ESP_MANT_SIST.docx
20200917_BCD_NORM_POLT_ESP_COMUNICAC_PERSONAS.docx
20210517_BCD_NORM_POLT_ESP_PERS.docx
20210525_BCD_NORM_POLT_ESP_RECOMPENSAS.docx
20200917_BCD_NORM_POLT_ESP_COOKIES.docx
20200917_BCD_NORM_POLT_ESP_PRIVACIDAD.docx
20201118_GRUPOBC_politica de protección de datos_2020.pdf
20200917_BCD_NORM_POLT_ESP_REL_TERC.docx
20210517_BCDIGITAL_NORM_POLT_ESP_REDES_SOCIALES.docx
20210917_BCD_NORM_POLT_ESP_REL_CLIENTE.docx

1_20200917_BCD_NORM_POLT_ESP_SEG_FIS.docx

20200917_BCD_NORM_POLT_ESP_CONT_ACCESOS.docx

20200917_BCD_NORM_POLT_ESP_SEG_LOG.docx

20210617_BCD_NORM_POLT_ESP_SERV_NUBE.docx

20200917_BCD_NORM_POLT_ESP_SW_EXPLOTACION.docx

20200917_BCDIGITAL_POLT_ESP_ENT_DES_SEG.docx

PROCEDIMIENTOS Y PLANES

20201015_BCDIGITAL_PLAN_FORMACION.xlsx

20201221_GBC_Contenido Formación Desarrollo Seguro

20201015_BCDIGITAL_GESTION_CN

20201015_bcdigital_gestion_crisis_v1

20201015_bcdigital_plan_cont_neg.pdf

20210701_BCDIGITAL_FORMACION CONTINUIDAD DE NEGOCIO.pptx

20220201_BCDIGITAL_FORM_CONCIENC Y SEGURIDAD DE LA INFORMACIÓN

20220201_BCDS_EFIC_FORM_DESARROLLO SEGURO

20210201_BCDIGITAL_PLAN_CONCIENCIACION_SEG_INF.xlsx