POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN
BCN CONSULTORES

Contenido

OBJETIVO

Las políticas de la Seguridad de la Información buscan establecer controles administrativos y operativos que regulen de manera eficaz el acceso de los usuarios a la información en BCN CONSULTORES, estableciendo lineamientos que buscan proteger la información generada por los procesos de BCN CONSULTORES y la tecnología utilizada para su procesamiento ante las amenazas del entorno, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de la información.

ALCANCE

La política de Seguridad de la Información aplica en todos los ámbitos de BCN CONSULTORES constituidos por colaboradores, proveedores, contratistas y las demás partes interesadas identificadas, que cuenten con el acceso a información a través de los diferentes canales, para el manejo de información en el **PROCESO DE CONSULTORÍA Y SOPORTE EN FACTURACIÓN ELECTRÓNICA**, relacionados con seguridad y privacidad de la información.

VIGENCIA

Las presentes disposiciones están vigentes a partir de la fecha de su firma y publicación.

DEFINICIONES

ACTIVO DE INFORMACIÓN: Es toda herramienta que CONSTRUYA, PROCESE, TRANSFIERA o ALMACENE INFORMACIÓN, que tiene valor para la organización debido a que es usado o interviene en alguna función directa o indirecta para BCN CONSULTORES o para el proceso a certificar.

AUDITORIA: Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluarla objetivamente para determinar hasta qué punto se cumplen los criterios de auditoría. (NTC – ISO/IEC 27000)

DISPONIBILIDAD: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. (NTC – ISO/IEC 27000)

CANALES DE COMUNICACIONES: Corresponde al medio utilizado para la transmisión de información.

CIFRADO: Que se encuentra trascrito en letras o símbolos, de acuerdo con una clave, para proteger su contenido, mediante un código o llave criptográfica.

CLAVES O CONTRASEÑAS: Corresponden a una serie de caracteres pertenecientes a un usuario con un login, usado con fines de identificar al usuario para la aprobación de ejecución de tareas.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. (NTC – ISO/IEC 27000)

CONTROLES CRIPTOGRÁFICOS: Son herramientas que se utilizan para cifrar información, protegiendo su contenido y dando el uso exclusivo a quien posea las llaves de cifrado o códigos.

CORREO ELECTRÓNICO: Es un servicio que permite la transmisión de mensajes electrónicos.

DISPONIBILIDAD: Propiedad de ser accesible y utilizable a solicitud de una entidad autorizada. (NTC – ISO/IEC 27000)

EQUIPOS DE CÓMPUTO: Es un elemento tecnológico tangible con un propósito específico en las labores de oficina, por ejemplo: computador, la impresora, el escáner, etc.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Son las acciones que violan las disposiciones del presente manual o las políticas, las cuales pueden generar una pérdida a los activos de información enfocado a la afectación de la Confidencialidad, Integridad y Disponibilidad.

EXTERNOS O TERCEROS: Toda empresa o persona que presta un servicio para la realización de funciones especiales diferentes a las del fondo (Ejemplo: Personal de vigilancia, personal de mantenimiento, personal de aseo, Revisoría, contraloría, etc.).

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Evento único o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información. (NTC – ISO/IEC 27000)

INTEGRIDAD: Propiedad de exactitud y completitud. (NTC – ISO/IEC 27000)

MEDIDAS DE SEGURIDAD: Son las medidas de seguridad para proteger la información sensible y confidencial de BCN CONSULTORES.

NORMA ISO 27001:2013: Es la versión del año 2013 de la norma ISO 27001 que "proporciona los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información." [Fuente: ISO 27001:2013].

NORMA ISO 27002:2013: Es la versión del año 2013 de la norma ISO 27002 que "está diseñada para que las organizaciones la usen como un marco de referencia para seleccionar controles dentro del proceso de implementación de un Sistema de Gestión de la Seguridad de la Información". [Fuente: ISO 27002:2013].

PARTE INTERESADA: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad. Una persona que toma decisiones puede ser una parte involucrada. [Fuente: ISO 31000].

POLÍTICA: Intenciones y dirección de una organización, según lo expresado formalmente por su alta dirección. (NTC – ISO/IEC 27000)

PROPIETARIO DE LA INFORMACIÓN: Es el rol asignado, entidad o unidad de negocio que ha aceptado la responsabilidad de la administración del activo de información y se encarga de su control, producción, desarrollo, mantenimiento, uso y seguridad.

RECURSOS TECNOLÓGICOS: Son aquellos elementos informáticos de los que dispone BCN CONSULTORES para su aprovechamiento como apoyo en las funciones requeridas para la gestión de sus procesos.

RED: Es un conjunto computadoras y/o dispositivos interconectados mediante cables, señales, ondas o cualquier otro medio de transporte de datos, que comparten información.

RIESGO: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de aquello que se espera, sea positivo, negativo o ambos. Los objetivos pueden tener aspectos diferentes (económicos, de imagen, medio ambiente) y se pueden aplicar a niveles diferentes (estratégico, operacional, toda la organización) [Fuente: ISO 31000].

SISTEMA DE GESTIÓN: Conjunto de elementos que interactúan y se interrelacionan para establecer políticas y objetivos y los procesos para alcanzar dichos objetivos.

SOFTWARE: Es el término usado para nombrar a los programas y/o aplicaciones que hacen posible que el usuario pueda interactuar con el computador.

SEGURIDAD DE LA INFORMACIÓN: Hace referencia a la preservación de la confidencialidad (propiedad de que la información, significa que no esté disponible o revelada a individuos no autorizados, entidades o procesos.), integridad (protección de la exactitud e integridad de los activos) y disponibilidad (propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada) de la información

VULNERABILIDAD: Debilidad identificada sobre un activo y que puede ser aprovechado por una amenaza para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

LLAVE CRIPTOGRAFICA: Herramientas, utilizadas en los procesos de cifrado para contener las claves mediante las cuales pueden descifrarse elementos previamente codificados.

POLITICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN[1]

BCN CONSULTORES dentro de su marco de visión contempla el generar, promover y ser parte de proyectos con ideas innovadoras que permitan el crecimiento y desarrollo de la empresa, sus clientes y del país.

Esta política se cimenta en los objetivos del Sistema de Gestión de Seguridad de la Información junto con las políticas adjuntas, y alineadas con el alcance del SGSI, fortalecerán la cultura interna en Seguridad de la Información y permitirán identificar y proteger los activos de información mediante la asignación de roles y responsabilidades, que contribuirán a desarrollar, implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI).

1. Velar por la protección de los activos de información en el marco de la triada de la Seguridad de la Información: La Confidencialidad, la Integridad y la Disponibilidad.

[1] Esta política y las demás incluidas en este documento serán sometidas a revisiones periódicas por parte de la Gerencia de BCN Consultores o quien estos designen, están propensas a cambios si existiesen y serán ajustadas según los requerimientos del Sistema de Gestión de Seguridad de la Información con enfoque al mejoramiento continuo.

2. Desarrollar un ejercicio adecuado de identificación, análisis y valoración de riesgos para asignar controles que ayuden en la mitigación de los riesgos identificados.
3. Proveer herramientas que ayuden en el ejercicio de Continuidad del Negocio en el marco del Sistema de Gestión de Seguridad de la información.
4. Promover una cultura de mejora continua con respecto al Sistema de Gestión de Seguridad de la información.

Para más información sobre los objetivos del SGSI remítase al documento SGSI-PLA-002 CONTEXTO DE LA ORGANIZACIÓN v4.

DEBERES

En el presente documento se exponen las diferentes políticas de uso, mantenimiento y protección de la información y elementos tecnológicos. Son complemento a la Política General de Seguridad de la Información de BCN CONSULTORES, y representan su visión en cuanto a la protección de sus activos de información y los de sus partes interesadas.

Por tanto, y según las directrices establecidas los incumplimientos a las Políticas y Controles de Seguridad de la Información serán reportados, registrados y monitoreados.

POLÍTICA DE INCUMPLIMIENTO

El cumplimiento de las Políticas de Seguridad de la información es obligatorio para todo empleado de BCN CONSULTORES y cualquier colaborador que tenga conocimiento de hechos que constituyan un incumplimiento al SGSI podrá reportarlo a través de los medios definidos para tal fin.

Todo incumplimiento a estas se considerará como un incidente de seguridad, será investigado y de acuerdo con la gravedad, se tomarán las acciones legales correspondientes, para lo cual BCN Consultores se reserva la facultad de iniciar los procesos a que haya lugar.

POLÍTICA PARA EL USO ADECUADO DE LOS ACTIVOS

El acceso a los documentos en formatos físicos y digitales mientras dure su ciclo de vida, estará determinado a la idoneidad del área o dependencia específica y a los permisos y niveles de acceso determinados por la gerencia de BCN CONSULTORES

Para el manejo de documentos cargados en la nube empresarial, la gerencia establecerá lo parámetros para asignación de privilegios de acceso a los colaboradores conforme a sus funciones y competencias.

En BCN Consultores se considera la información como un activo fundamental y es por esta razón que se implementaran los mecanismos necesarios que garanticen y promuevan la Integridad, Confidencialidad y Disponibilidad de la información.

Los colaboradores de BCN Consultores son responsables de almacenar la información que necesita de respaldo en los espacios definidos para tal fin y deberán protegerla según las medidas adoptadas que eviten el acceso de personal no autorizado teniendo en cuenta las directrices registradas en el marco del SGSI.

Aquellos colaboradores que hagan uso de información catalogada como confidencial, deberán firmar un “acuerdo de confidencialidad” consignado en su contrato, donde se comprometan a no divulgar y utilizar la información respetando los niveles establecidos para su clasificación; y toda violación a lo establecido en este acuerdo será considerado de manera inmediata como una falta grave y tratada como un “incidente de seguridad”.

Para más información al respecto puede consultar SGSI-GUI-003 apartado INVENTARIO DE ACTIVOS DE INFORMACIÓN

POLÍTICA DE USO DE LOS RECURSOS TECNOLÓGICOS

BCN CONSULTORES establece las normas para el uso de recursos tecnológicos como parte de las herramientas de trabajo (Software, Equipos de cómputo, teléfono móvil, redes, enlaces de comunicaciones, etc.) para uso de sus colaboradores y de todo tercero autorizado para hacerlo en el marco de las disposiciones establecidas en el Sistema de Gestión de Seguridad de la Información con el fin de promover la Integridad, Confidencialidad y Disponibilidad de la información y su uso queda sujeto a las siguientes condiciones:

- No está permitida la utilización de los recursos facilitados por la compañía para fines comerciales, recreativos o que salgan del contexto de la razón social de BCN Consultores.
- Los colaboradores de BCN CONSULTORES son quienes cuentan con derechos exclusivos de los recursos y son responsables de su utilización y del uso de la

información que contengan conforme a la Política para el Uso Adecuado de los Activos. Dichos derechos serán revocados en el momento de la terminación de su contrato o por orden de la Gerencia General.

- Para los computadores se deberán tomar medidas de seguridad cuando no estén en uso.
- Se deberá realizar cambio de contraseñas cuando el sistema así lo indique, cumpliendo con el estándar para contraseñas establecido.
- Los computadores deben contar con un antivirus debidamente licenciado.
- Los computadores no se deben dejar manipular por personas externas a BCN CONSULTORES.
- Está prohibida la utilización de programas externos para interferir con las sesiones de los computadores sin previa autorización.
- Los colaboradores deberán poner en conocimiento de su superior en caso de conectar medios de almacenamiento removibles de terceros no autorizados, tales como CD's, DVD's, memorias USB y discos duros externos.
- La instalación de cualquier tipo de software en los equipos de cómputo de BCN CONSULTORES debe ser hecho bajo requerimiento de las necesidades laborales y con la autorización del superior inmediato.
- No se deben descargar archivos ejecutables de Internet sin antes validar su propósito y fabricante.
- Los colaboradores que no pertenezcan al área de Tecnología no deben realizar cambios en relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla.
- Cualquier conexión remota al equipo del empleado deberá ser informada, supervisada y autorizada por el jefe inmediato.
- Los colaboradores tienen la responsabilidad de las impresiones que se envíen y deberán comprobar y recoger las que fueron impresas. Está prohibido dejar impresiones erróneas sobre la mesa de las impresoras, ni en los puestos de trabajo de las personas cercanas a ella, ni en la impresora.
- El uso negligente de los recursos informáticos que causen daño parcial o total a la información de BCN CONSULTORES será causal de terminación de contrato y dependiendo del caso, de sanciones jurídicas.

POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

Los activos de información de BCN CONSULTORES, serán sometidos a un proceso de identificación y posterior clasificación con el fin de establecer las opciones de disposición y protección necesarias en el Marco del Sistema de Gestión de Seguridad de la información.

La escala de clasificación de la información considerará el valor de esta para BCN CONSULTORES, por lo que los controles serán más estrictos con la información de mayor valor con el fin de garantizar su confidencialidad, Integridad y Disponibilidad. En caso de una requerir difusión de la información, se evaluarán las razones por las cuales se deban o no realizar y de adoptarán las medidas necesarias para tal fin.

Toda información debe tener asignado un propietario, quien será la persona encargada de propender por su clasificación teniendo en cuenta las siguientes definiciones:

CLASIFICACIÓN	DESCRIPCIÓN	NIVEL DE PROTECCIÓN
Confidencial	Información propia de BCN CONSULTORES, acceso a sistemas de información, llaves criptográficas, certificados digitales de los clientes e información de cumplimiento de la ley.	Alto
Restringida	Información clasificada de clientes y colaboradores que solo debe ser accedida por personal autorizado para ello, previa autorización del dueño del proceso.	
Interna	Información que no debe ser conocido por el público en general y es sólo de interés de los colaboradores.	Medio
Pública	Información de interés de personal externo a BCN CONSULTORES.	Bajo

Para más información al respecto puede consultar SGSI-GUI-003 apartado CLASIFICACIÓN DE LA INFORMACIÓN

POLÍTICA DE USO DE INTERNET

El objetivo de BCN Consultores con respecto a la Política de uso de internet es ayudar en la realización de las labores contratadas ofreciendo el acceso a Internet a colaboradores y clientes, los cuales deben asumir los lineamientos definidos para tal fin.

Esta política define las acciones que permiten reducir los riesgos que se puedan presentar por el uso de Internet (redes privadas o públicas), los cuales pueden comprometer la triada de la información (integridad, disponibilidad y confidencialidad) y dictamina que los privilegios de acceso a Internet serán asignados conforme a la necesidad y funciones de los colaboradores

de BCN CONSULTORES, con lo cual se definen las siguientes condiciones de uso. Cualquier propósito ajeno a las funciones estrictamente laborales serán restringidas.

BCN CONSULTORES podrá controlar, verificar y hacer monitoreo sobre el uso adecuado de este recurso. A continuación, se listan las restricciones definidas:

- El acceso a páginas relacionadas con apuestas, pornografía y drogas está estrictamente prohibido.
- Los colaboradores no deben abrir, ni revisar correos electrónicos considerados inseguros, por el riesgo latente de contener mensajes de dudosa procedencia o archivos contaminados con virus que pueden perjudicar la red de BCN CONSULTORES, fugas de información, ransomware, entre otros.
- No se permitirá la descarga, uso, intercambio e instalación de productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables, herramientas de hacking, entre otros.
- El servicio de Internet podrá ser utilizado para uso personal de manera ética, y responsable, sin afectar la productividad ni la protección de la información de BCN CONSULTORES
- Los servicios de la nube son una herramienta de trabajo de BCN CONSULTORES, es responsabilidad de sus colaboradores la utilización de ésta de forma responsable de acuerdo con los lineamientos de la Gerencia General. Queda totalmente prohibido ceder su uso a personas no vinculadas a BCN CONSULTORES.
- Los equipos que cuentan con internet pueden ser sometidos a auditorías sin previo aviso con el fin de garantizar el buen uso de este.
- Está prohibida la instalación de programas para entretenimiento: música (MP3, RA, WAV); emisoras de radio vía Internet. (Winamp, REAL AUDIO, MUSIC MATCH, Oozic PLAYER); para ver vídeos o emisoras de televisión vía Internet. (REAL AUDIO, BWV, etc.). (Este punto aplica para uso de red corporativa)
- No se puede realizar ningún tipo de compras a través del internet institucional.

En caso de que un colaborador de BCN Consultores sea encontrado haciendo mal uso del Internet, se reportara la situación presentada al Jefe Inmediato y al oficial de Seguridad de la Información con el fin de adoptar las medidas a que haya lugar.

POLÍTICA DE USO DEL CORREO ELECTRÓNICO

El correo electrónico es una herramienta tecnológica proporcionada por BCN CONSULTORES, por medio del cual se apoyan las actividades de sus colaboradores y se establece como el

principal medio de la comunicación, por lo que el uso inapropiado de éste expone a BCN CONSULTORES a riesgos informáticos que pueden comprometer a la firma de manera reputacional y hasta legal, como consecuencia de una mala comunicación, por lo cual cada empleado de BCN CONSULTORES debe ser responsable de su utilización y conocimiento de las respectivas restricciones y condiciones de uso.

- BCN CONSULTORES podrá realizar, y sin previo aviso, auditorías sobre el uso adecuado de este recurso.
- Los colaboradores deberán utilizar este recurso específicamente con fines empresariales y no deberá ser registrado en formularios de páginas que no correspondan a partes interesadas de BCN CONSULTORES.
- Se debe evitar enviar información personal o de BCN CONSULTORES a buzones de proveedores desconocidos
- El contenido de los buzones de correo es de propiedad de BCN CONSULTORES
- No se podrán enviar o reenviar cadenas de correo, SPAM, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.
- El envío de información **CONFIDENCIAL** se realizará por medios seguros.
- Los mensajes con documentos adjuntos deberán venir de un destinatario conocido. Si se presentara algún tipo de duda acerca de mensajes recibidos se deberá informar a la gerencia para su validación.
- Todos los mensajes enviados deberán respetar el estándar de formato e imagen corporativa definido por BCN CONSULTORES y deberán conservar en todos los casos el mensaje legal corporativo.
- No se debe utilizar el correo empresarial para enviar mensajes personales u ofensivos, injuriosos, cadenas de mensajes o mensajes que se relacionen con actividades ilegales y no éticas, o que atenten contra el buen nombre de la organización.
- En caso de que un empleado tome vacaciones o presente ausencia por un tiempo considerable, deberá informar al administrador para dejar un mensaje de tipo informativo, o redireccionar los correos a otra cuenta que su superior directo autorice.

POLÍTICA DE ESCRITORIO Y PANTALLA DESPEJADA

Esta política establece buenas prácticas para el orden y la limpieza en los puestos de trabajo de los colaboradores de BCN CONSULTORES y da cumplimiento a directrices de Seguridad de la Información que están enmarcadas en la manera en que se manejan los activos de BCN Consultores que estén a cargo de un propietario de un activo de la Información.

En el marco del SGSI, es fundamental la protección de la información con el fin de evitar el acceso de personas diferentes a aquellas que hacen uso de la misma, por lo que en vista que se reciben visitantes en el lugar de trabajo, se hace necesaria la implementación de buenas prácticas relacionadas con el mantenimiento del espacios de trabajo (Escritorio y Equipo de cómputo) lo más limpios y organizados posible, y de esta manera controlar los activos de información a cargo y evitar incidentes de seguridad.

Los colaboradores con activos a su cargo serán responsables de los mismos, mientras tengan la información a su cargo, por lo que deben de mantener niveles de protección en el marco del SGSI haciendo uso adecuado de los recursos, por lo cual se dan las siguientes directrices:

Para el puesto de trabajo:

- Los colaboradores tienen la responsabilidad de mantener sus puestos de trabajo limpios y ordenados, manteniendo los implementos necesarios para cumplir con las funciones inherentes a su cargo.
- Las comidas y bebidas se consumirán en los lugares destinados para ello.
- Cuando finalice la jornada laboral, los colaboradores deberán almacenar los documentos con información sensible en los lugares determinados para ello.
- En los puestos de trabajo de los colaboradores deben existir medidas de seguridad física y digital tendientes a la protección de la información que impidan el acceso libre por parte de personas externas.
- Queda prohibido el almacenamiento de contraseñas en notas autoadhesivas.

Para pantalla despejada:

- La pantalla del computador solo debe contener los accesos directos a las aplicaciones autorizadas para el normal desarrollo de las funciones de los colaboradores de BCN Consultores
- La pantalla de los computadores deberá ser configurada para bloquearse automáticamente como máximo a los 30 minutos de inactividad y cada colaborador

deberá bloquear la pantalla una vez se levanta de su escritorio mediante las teclas Windows + L.

- Las pantallas de los computadores deberán estar ubicadas de manera que personal externo a BCN CONSULTORES no sea visible fácilmente.
- Los colaboradores no deberán dejar desatendidos sus dispositivos móviles.
- La gerencia será responsable de verificar los controles necesarios para asegurar que sólo los colaboradores autorizados puedan hacer uso de los medios de almacenamiento removibles.

Todo empleado de BCN CONSULTORES está en obligación de informar cualquier incumplimiento a esta política o cuando considere que no se está cumpliendo con la confidencialidad, integridad y disponibilidad de la información.

POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO

Esta política brinda un marco de referencia para el control de acceso físico a las áreas donde se mantiene o se almacena información sensible, donde se encuentren computadores con información crítica e infraestructura que soporta la operación de BCN CONSULTORES.

En este orden de ideas en BCN Consultores se propende por el mantenimiento de la Confidencialidad, Integridad y Disponibilidad de la información por lo que, tanto colaboradores como visitantes deben tener presentes las siguientes indicaciones:

Condiciones generales:

- No se autorizará a los visitantes el acceso a las instalaciones de BCN CONSULTORES por fuera de los horarios laborales establecidos, o a menos que haya un empleado que lo apruebe, quien será responsable por el visitante durante su permanencia en las instalaciones de BCN CONSULTORES
- Todo visitante deberá ser registrado en el formato que se haya designado para tal fin.
- Todas las áreas de procesamiento de información clasificado como confidencial o restringido deben contar con protecciones a nivel físico y deben cubrir las necesidades en cuanto a controles de entrada físicos y protección contra amenazas ambientales. Sus correspondientes controles deben ser de acuerdo con la necesidad de aseguramiento, clasificación y valoración de los activos de información establecidos por los responsables
- Se deben identificar las salidas de emergencia y asignar a un brigadista, quien deberá conocer el plan de emergencias del edificio.

- No dejar abandonada en las impresoras información Confidencial y Restringida, una vez se haya impreso

En la Oficina:

- La oficina cuenta con extintores de polvo químico seco (Solkaflam), los cuales serán utilizados en caso de una emergencia.
- Los computadores y equipos eléctricos deben estar protegidos contra fallas de energía para asegurar la continuidad del servicio.
- Es responsabilidad de todos los colaboradores bloquear la sesión de trabajo en su equipo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario.
- Al final de la jornada laboral, se deben cerrar todas las aplicaciones y dejar los equipos apagados.
- A pesar de que en BCN Consultores se está trabajando en la implementación de “Cero Papel”, en caso de requerir impresiones, se debe velar por no dejar en las impresoras información clasificada como Confidencial.

Suministro Eléctrico:

- Al interior de las instalaciones de BCN Consultores se debe contar con múltiples líneas de suministro de energía eléctrica regulada.

Cableado estructurado:

- Se debe dar cumplimiento a los requisitos Técnicos vigentes para tal fin.
- Las Conexiones deben ser adecuadas para el respectivo uso ya sea de Energía Eléctrica o de Datos y estas deberán estar separadas.
- El Cableado será protegido contra Intercepción no Autorizada

Amenazas externas:

- Las oficinas de BCN Consultores o los accesos a estas deben contar con sistemas de alarmas y cámaras de seguridad, sistema de detección y extinción de incendios.
- Los equipos de cómputo deben estar aislado de amenazas como fuego, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

POLÍTICA DE CONTROL DE ACCESO Y CONTRASEÑAS

Con el objetivo de garantizar que la información, las redes de datos, los recursos tecnológicos y las áreas en las cuales se procesa y se gestiona información, cuente con la debida protección

frente a accesos físicos y lógicos catalogados como indebidos se promueve la política de control de acceso y contraseñas en BCN Consultores.

Los colaboradores de BCN CONSULTORES deberán seguir las siguientes políticas para garantizar un adecuado control de acceso y uso de las contraseñas de acceso de computadores, sistemas de información y otros relacionados que puedan poner en riesgo la Seguridad de la Información.

- Los propietarios de los activos de la información serán las personas responsables de clasificar la información, determinar los controles de acceso, autenticación y utilización que se van a implementar, aprobar o denegar la solicitud de asignación de privilegios de acceso a su información y su revisión correspondiente.
- Las contraseñas son de uso personal de cada uno de los colaboradores de BCN CONSULTORES y por ningún motivo deberán ser utilizadas por personas diferentes.
- Al momento de crear una contraseña no se debe incluir información personal como, por ejemplo: Nombres de familiares, mascotas, meses, ciudades, equipos, programas de televisión, libros, etc.
- Las contraseñas no deberán ser reveladas por vía telefónica, correo electrónico o por ningún otro medio.
- Reportar cualquier sospecha de que otra persona esté utilizando su contraseña o usuario asignado.
- Reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece.
- BCN CONSULTORES definirá e implantará controles para proteger la información propia y de sus clientes contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos.
- La asignación de acceso a los servicios de red será autorizada por la Gerencia, así como el acceso y su nivel de acceso a la información contenida en la nube empresarial.

Para más información al respecto puede consultar IT-PRO-002_CONTROL Y CAMBIO DE CONTRASEÑAS

POLÍTICA DE COPIAS DE RESPALDO

BCN Consultores en el marco el Sistema de Gestión de Seguridad de la Información, identificó la necesidad de contar con la Política de Copias de Respaldo de tal manera que se pueda garantizar la Confidencialidad, la Integridad y la Disponibilidad de la información crítica.

El objetivo de la Política es definir las directrices generales aplicables tanto a la infraestructura tecnológica como a los activos y sistemas de información crítica para el normal desarrollo de las labores contratadas tanto internas como externas.

En este orden de ideas, todos los colaboradores deben configurar el Drive para sincronizarse automáticamente con su equipo de cómputo y dependiendo del cargo, el empleado deberá sincronizar todo el disco duro o la información pertinente a sus funciones.

POLÍTICA DE INCIDENTES DE SEGURIDAD

Con el objetivo de identificar incidentes o brechas de seguridad en la información de BCN Consultores, se define los mecanismos necesarios para el reporte oportuno de estas vulnerabilidades y su respectiva gestión, para lo cual, todos los incidentes o eventos de seguridad ocurridos en BCN CONSULTORES deberán ser reportados a la Gerencia o a quien asume el rol de Oficial de Seguridad de la Información, con el fin de determinar sus causas y responsables. Teniendo en cuenta la gravedad, se decidirá si se contacta un aliado para asistir en la investigación. Según las responsabilidades identificadas, se definirán planes de acción y se iniciarán las sanciones disciplinarias correspondientes.

Es responsabilidad de todos los colaboradores de BCN CONSULTORES reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

BCN CONSULTORES podrá por medios propios o a través de un tercero utilizar herramientas automatizadas de monitoreo y búsqueda de evidencia física y/o digital que indiquen uso no adecuado de los recursos de BCN CONSULTORES por parte de los funcionarios y contratistas.

Para más información al respecto puede consultar SGSI-PRO-007_GESTIÓN DE INCIDENTES

POLÍTICA DE ACUERDOS DE CONFIDENCIALIDAD

El objetivo de esta política es generar directrices que permitan evitar la divulgación de información ya sea accidental o de manera intencionada que pueda generar afectación a BCN Consultores.

Por lo anterior y en el marco del SGSI, todos los colaboradores de BCN CONSULTORES, como parte del proceso de contratación, deberán aceptar los acuerdos de confidencialidad definidos

en sus correspondientes contratos de trabajo mediante una cláusula, la cual indica los compromisos de protección y el buen uso de la información de acuerdo con los criterios establecidos por la Gerencia.

De igual manera se podrá establecer acuerdo de confidencialidad con clientes y proveedores en los cuales se deben definir compromisos de protección y el buen uso de la información de acuerdo con los criterios establecidos por la Gerencia.

Para más información al respecto puede consultar SGSI-PRO-003_REVISIÓN DE CLÁUSULAS DE CONFIDENCIALIDAD

POLÍTICA DE ELIMINACIÓN Y DESTRUCCIÓN

Para BCN CONSULTORES es importante el mantenimiento del SGSI por lo que en este orden de ideas y con el objetivo de definir lineamientos para la correcta disposición de documentación se definen los lineamientos generales para eliminar documentación clasificada como sensible.

La información que será sometida a eliminación, y de acuerdo a su criticidad, siguiendo las recomendaciones el Decreto 805 del 24 de abril de 2013 (que modifica el artículo 56 del Código de Comercio), que indica que "*todas las empresas tienen la obligación de conservar los libros y la documentación, por los medios que le facilita la ley, por un periodo mínimo de diez (10) años, término a partir del cual cesa la obligación; por ende, nada obsta para proceder a la su destrucción, sin perjuicio que con posterioridad decidan continuar conservándolos*", será toda aquella que clasifique como obsoleta, aquella que haya pasado el período legal obligatorio de reclamaciones y aquella que carezca de valor, sometiendo su correspondiente eliminación por medio de medios y herramientas que garanticen su destrucción y borrado seguro, sea el caso.

Dichos acuerdos deberán ser divulgados con los colaboradores de manera oportuna y estos a su vez están en la obligación de cumplir y hacer cumplir las directrices definidas por BCN Consultores para tal fin.

POLÍTICA TRAE TU PROPIO DISPOSITIVO (BYOD)

Para BCN CONSULTORES, la continuidad del negocio y la necesidad de mantener un contacto con colaboradores, clientes y proveedores ha generado la necesidad de brindar a sus colaboradores la posibilidad de traer su propio dispositivo móvil (teléfono celular), mientras se dé cumplimiento a lo dispuesto en la "Política de uso de los recursos tecnológicos".

En este orden de ideas se tienen las siguientes disposiciones que van en vía de promover la Confidencialidad, la Integridad y Disponibilidad de información:

- Los colaboradores pueden llevar sus propios dispositivos móviles al lugar de trabajo y hacer uso de ellos para desempeñar sus funciones.
- Los colaboradores serán responsables de la instalación de paquetes y parches requeridos por el sistema operativo en los dispositivos de cómputo y móviles, al igual que su licenciamiento, con el fin de fomentar y mantener la uniformidad como buena práctica.
- Si un empleado pierde su dispositivo móvil, la información de BCN CONSULTORES allí contenida deberá figurar en un repositorio en la nube, como lo dicta la “Política de Transferencia de información” y el hecho será reportado como un incidente de seguridad.
- Cualquier otro tipo de información existente será responsabilidad del empleado.
- El empleado es responsable del uso adecuado de su dispositivo móvil y de la información allí almacenada y en caso de utilizarlo en el ejercicio de sus funciones, acepta las directrices asociadas con las políticas de SGSI establecidas, sin que esto vaya en contra de su privacidad.

Para más información al respecto puede consultar SGSI-GUI-003_Guia para el uso adecuado de Recursos Tecnológicos apartado TELEFONOS (EQUIPOS MOVILES).

POLÍTICA DE TELETRABAJO

Esta política tiene por objeto establecer las condiciones en las cuales los colaboradores de BCN Consultores realizarán las actividades relacionadas con el trabajo desde su hogar de forma temporal cuando las circunstancias dificulten la asistencia presencial a las instalaciones de BCN Consultores.

- Si el empleado se encuentra en modalidad de teletrabajo, éste utilizará las herramientas tecnologías y de comunicaciones provistas por BCN CONSULTORES para el respaldo de la información de esta.
- Todos los colaboradores y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- El empleado que se vaya a conectar deberá informar a su jefe inmediato, el cual deberá mantener un registro de conexiones y actividades realizadas fuera de las instalaciones.
- Velar por confidencialidad de la información

- Uso de auriculares para que no sea escuchado por terceros
- Queda rotundamente prohibida la realización de impresiones
- Revisar el tema de la inclusión de firma digital en Política de uso adecuado de recursos tecnológicos
- Es requerido que lo equipos suministrados (para uso en las instalaciones o en trabajo en casa) sean bloqueados cuando no estén bajo supervisión del colaborador, sin embargo, el tiempo de bloqueo automático se debe configurar con un máximo de 30 minutos acorde a la necesidad de cada colaborador.
- Con el ánimo de mantener un ambiente controlado durante el "trabajo en casa" se requiere de medidas que garanticen la confidencialidad de la información
- Los miembros del núcleo familiar, visitantes al sitio de trabajo remoto no deben acceder a los activos de información (Equipo de Cómputo y dispositivo Móvil) y el colaborador debe garantizar que los anteriormente mencionado no hagan uso de estas herramientas.
- El monitor debe ser ubicado de manera tal que nadie contrario al colaborador tenga vista del monitor de tal manera que evite que personal no autorizado pueda ver la información que se encuentre desplegada.

Seguridad del equipo Fuera de BCN Consultores

- El uso de equipos de cómputo, portátiles, discos removibles destinado al procesamiento de información, fuera de las instalaciones de BCN Consultores, será autorizado por el responsable del proceso al que pertenezca el colaborador.

- El colaborador que está autorizado a retirar un equipo de cómputo o portátil debe tener el mismo nivel de protección de la información como si estuviese en las instalaciones de BCN Consultores.

Todo colaborador de BCN Consultores deberá utilizar los canales de comunicación designados por la empresa para mantener el contacto con el equipo de trabajo y con los clientes, teniendo en cuenta las siguientes condiciones:

- En el caso de conversaciones telefónicas, se recomienda utilizar espacios cerrados en los cuales la conversación no pueda ser escuchada por terceros.
- En el caso de sesiones virtuales, se recomienda utilizar aplicaciones de confianza y que ofrezcan medidas de seguridad suficientes.

- Los correos electrónicos dirigidos a miembros de la organización o a clientes deberán ser remitidos desde la dirección de correo asignada por BCN Consultores.
- Queda prohibido, salvo autorización en contrario, el uso de páginas web o aplicaciones desarrolladas por terceros que no cuenten con protocolos de seguridad suficientes.
- Evitar el uso de Redes Sociales u otras plataformas públicas para compartir información confidencial o protegida por propiedad intelectual.

Dichos acuerdos deberán ser aceptados como parte del proceso de contratación.

POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

El intercambio de información clasificada como sensible entre BCN CONSULTORES y terceras partes u otras empresas deberá, realizarse de forma controlada y en los contratos con empresas o terceros se deberán incluir acuerdos de confidencialidad de la información, acordes con el cumplimiento de la normatividad vigente nacional e internacional para el tratamiento de la información que así corresponda.

Dicha transferencia deberá establecerse de común acuerdo, definiendo los mecanismos que se van a utilizar con el fin de evitar la interceptación, copiado, modificación y/o destrucción de la información garantizando así la Confidencialidad, Integridad y Disponibilidad de la Información.

Los controles que se aplicarán serán los siguientes:

- Para información física, esta irá en un sobre sellado y etiquetado como Información Confidencial, utilizando medios de embalaje, de forma que esta información pueda estar protegida, si es el caso, contra golpes o daños.
- Se deberán usar servicios de mensajería fiables.
- El envío de información por medios electrónicos clasificada como sensible, y dado el caso, deberá ser enviado por medio de herramientas certificadas como correo seguro o por medio de archivos cifrados o con contraseña.
- Si la transferencia de la información se realiza por medios extraíbles como USB y discos duros externos, ésta deberá ser cifrada mediante algoritmos fuertes y confiables.
- Los colaboradores de BCN CONSULTORES no deberán revelar información sensible de proyectos por medios telefónicos.
- Los colaboradores de BCN CONSULTORES deben evitar mantener conversaciones de carácter confidencial en oficinas abiertas y lugares públicos.

La fuga de información puede ser sujeto de sanciones que podrían dar lugar a la terminación del contrato de trabajo y acciones legales, según las leyes vigentes.

POLÍTICA DE SEGURIDAD PARA PROVEEDORES Y/O VISITANTES

BCN CONSULTORES adoptará medidas de seguridad para salvaguardar los principios de la Seguridad de la Información en cuanto al manejo de activos de información y garantizará una adecuada gestión de aquellos activos clasificados como Confidenciales por medio de los siguientes controles alineados a la norma ISO 27001:2013.

- Aquellos proveedores que requieran el ingreso a las instalaciones de BCN CONSULTORES deberán registrarse en la recepción y esperar allí la correspondiente autorización de ingreso.
- El ingreso de dispositivos electrónicos es responsabilidad de cada proveedor de servicios, al igual que toda licencia de software que requiera.
- Todo proveedor deberá dar cumplimiento a los acuerdos de confidencialidad, SGSI y demás políticas establecidas para el intercambio comercial con terceros.
- Todo proveedor deberá ser recibido y contar con acompañamiento por un empleado asignado desde su ingreso hasta salir de las instalaciones de BCN CONSULTORES
- Para el intercambio de información se deberá tener en cuenta cumplir con los protocolos indicados en la “Política de transferencia de Información”, garantizando de esa forma la integridad, disponibilidad y confidencialidad de la información.

Todos los proveedores de BCN CONSULTORES deben aceptar los acuerdos de confidencialidad definidos, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos. Sea el caso, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de BCN CONSULTORES a personas o entidades externas.
Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

El no cumplimiento de las cláusulas de confidencialidad puede ser sujeto de sanciones que podrían dar lugar a la terminación del contrato de trabajo y acciones legales, según las leyes vigentes.

POLÍTICA DE CONTROLES CRIPTOGRAFICOS

Los colaboradores de BCN CONSULTORES, deberán tener en cuenta las siguientes directrices de uso de herramientas de cifrado y/o controles criptográficos que permitan la protección y salvaguarda de la información de todas las partes interesadas, en el proceso de Facturación Electrónica.

- La información que contenga contraseñas de usuario o claves para el control de acceso a los sistemas de información, deberá hacer uso de controles criptográficos y deberá ser almacenada cifrada o codificada.
- Todos los documentos deberán ser tratados y almacenados de acuerdo con la política de clasificación de la información una vez hayan sido cifrados y descifrados.
- Se deberá identificar todo sistema de información que requiera transmisión de información para que cumpla con la política de clasificación de la información, y que esta se encuentre protegida por los controles criptográficos establecidos.
- Los discos duros de los equipos de cómputo de escritorio, portátiles deberán ser cifrados, sí contienen información que deba ser protegida, según la política de clasificación de la información.
- Las llaves criptográficas deberán ser administradas por los dueños de la información o quienes hayan sido delegados por estos, según la política de clasificación de la información.

POLÍTICA DE TRATAMIENTO DE DATOS

BCN Consultores como responsable del tratamiento de datos personales obtenidos en desarrollo de su misionalidad y según lo contenido en la Ley 1581 de 2012 dispone la siguiente política de tratamiento de datos personales. Para todo lo relacionado con el tratamiento de datos personales el responsable será:

NOMBRE	BCN CONSULTORES COLOMBIA SAS
NIT	9011372265
DIRECCIÓN	Edificio Business Center, calle 116 #23-06, Oficina 311.
TELÉFONO	(571) 6945085

CORREO ELECTRÓNICO	soporte.colombia@bcncons.com

Teniendo en cuenta que BCN Consultores recolecta información a través de diferentes medios, se establece que la finalidad de los datos recolectados será única y exclusivamente para promover el adecuado registro, administración y veracidad de la información.

En este orden de ideas, la información en caso de que se requiera será suministrada a los siguientes grupos de personas:

- A las entidades que en ejercicio de sus funciones legales o por orden judicial lo requieran.
- A los terceros autorizados por el titular o por la ley.

Y sin perjuicio de las excepciones previstas en la ley, el titular de los datos personales debe dar su autorización previa, expresa e informada para su tratamiento, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior

CONTROL DE VERSIONES Y CAMBIOS

Versión	Fecha aprobación	Nota de cambio	Elaboró	Aprobó
1.0	02-03-2020		Jonathan Zamudio	Cristian Jiménez
2.0	17-07-2020	Ajuste Nemotecnia e inclusión de vigencia	Jonathan Zamudio	Cristian Jiménez
3.0	03-08-2020	Se incluye referenciación cruzada al contexto de la organización	Jonathan Zamudio	Cristian Jiménez
4.0	07-08-20	Inclusión de política de controles criptográficos y mejora en otras políticas	Jonathan Zamudio	Cristian Jiménez
5.0	11-05-2021	Se incluyen objetivos de SGSI. Se ajustan textos asociados a las Políticas de SGSI	Juan Pablo Meléndez Zabaleta	Felipe Escobar

		Se incluye la Política de Protección de Datos		