POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BOSTON INTERNATIONAL SCHOOL

1. INTRODUCCIÓN

Nuestra comunidad Boston está compuesta por personal administrativo, docentes, alumnos, padres de familia y familiares, una de las formas para interactuar y comunicarnos lo hacemos por medio de la tecnología, captura de datos y de información que nos es necesaria para lograr una muy buena gestión para todos los procesos, se hace necesario colocar reglas y políticas que nos permitan salvaguardar dicha información para lograr un buen manejo de esos datos.

2. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información de la institución BOSTON INTERNATIONAL SCHOOL, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

3. ALCANCE

La presente Política de Seguridad de la Información se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico de la institución debe ser conocida y cumplida por toda la comunidad REDBOSTON, personal administrativo, docentes, alumnos, padres de familia y familiares.

4. Términos y Definiciones

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la institución y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: es un documento en los que las directivas y diferentes departamentos de la institución manifiestan su voluntad de mantener la confidencialidad de la información del institución, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planning: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y

techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes al instituto.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Intitucion.

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del

instituto. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el la institución de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

Guías de clasificación de la información: directrices para catalogar la información de la entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de

seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencia, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

5. Políticas de la seguridad de Información

La información es un recurso que, como el resto de los activos, tiene valor para la institución y por consiguiente debe ser debidamente protegida. Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad del sistema, minimizando riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la institución . Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades de la institución para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información de la institución y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información. Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales. Mantener la Política de Seguridad de la institución actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Esta Política se aplica en todo el ámbito de la institución , a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

Responsabilidad

Jefes Administrativos, Jefe de sistemas o personal técnico y sea cual fuere su nivel jerárquico son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo. La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la institución, en cualquier área que se desempeñe. Las máximas autoridades de la Institución aprueban esta Política y son responsables de la autorización de sus modificaciones.

Compromiso

- La revisión y aprobación de las Políticas de Seguridad de la Información contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los funcionarios de la entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

Área de Recursos Humanos o quien desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad.

Área Tecnológica cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la institución . Por otra parte tendrá la función de efectuar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas en todas las fases.

Área Legal verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la institución con sus empleados y con terceros. Asimismo, asesorará en materia legal a la institución, en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente.

6. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad de la Información pretenden instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores de la institución . Por tal razón, es necesario que las violaciones a las Políticas de Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

7. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

La institución establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información. Normas que rigen para la estructura organizacional de seguridad de la información

Normas dirigidas a: DIRECCION

La Dirección del BOSTON INTERNATIONAL SCHOOL debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

La Dirección debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.

La Dirección debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.

La Dirección debe promover activamente una cultura de seguridad de la información en el instituto.

La Dirección debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.

La Dirección, debe asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la institución.

Normas dirigidas a: COMITÉ DE SEGURIDAD DE LA INFORMACION

El Comité de Seguridad de la Información debe actualizar y presentar ante la Junta Directiva las Políticas de Seguridad de la Información, la metodología para el análisis de riesgos de seguridad y la metodología para la clasificación de la información, según lo considere pertinente.

El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

El Comité de Seguridad de la Información debe verificar el cumplimiento de las políticas de seguridad de la información aquí mencionadas.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la institución. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: TODOS LOS USUARIOS

Administrativos, docentes, usuarios o personal provisto por terceras partes que realicen labores en o para el BOSTON INTERNATIONAL SCHOOL , tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

8. POLÍTICA PARA USO DE DISPOSITIVOS DE CÓMPUTO Y MÓVILES

El BOSTON INTERNATIONAL SCHOOL proveerá las condiciones para el manejo de los dispositivos de cómputo (portátiles, teléfonos inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios de la institución. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

Normas para uso de dispositivos de computo y móviles

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe investigar y probar las opciones de protección de los dispositivos de cómputo, móviles institucionales y personales que hagan uso de los servicios provistos por la institución.

La Dirección de Tecnología debe establecer las configuraciones aceptables para los dispositivos de computo móviles institucionales o personales que hagan uso de los servicios provistos por el BOSTON INTERNATIONAL SCHOOL

La Dirección de Tecnología debe establecer un método de bloqueo (por ejemplo, contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar estos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá el método de desbloqueo configurado.

La Dirección de Tecnología debe activar la opción de cifrado de la memoria de almacenamiento de los dispositivos de cómputo, móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

La Dirección de Tecnología debe configurar la opción de borrado remoto de información en los dispositivos de computo móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

La Dirección de Tecnología debe contar con una solución de copias de seguridad para la información contenida en los dispositivos de cómputo móviles institucionales de institución dichas copias deben acogerse a la Política de Copias de Respaldo de la Información.

La Dirección de Tecnología debe instalar un software de antivirus tanto en los dispositivos de cómputo móviles institucionales. como en los personales que hagan uso de los servicios provistos por el instituto

La Dirección de Tecnología debe activar los códigos de seguridad de la tarjeta SIM para los dispositivos de cómputo móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios deben evitar usar los dispositivos de cómputo móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos de cómputo móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.

Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos de cómputo y móviles institucionales.

Los usuarios deben, cada vez que el sistema de sus dispositivos de cómputo móviles institucionales notifique de una actualización disponible, no aceptar ni aplicar la nueva versión.

Los usuarios deben evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

Los usuarios deben evitar conectar a los dispositivos de computo y móviles institucionales asignados dispositivos por USB que no sean de la institución.

Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos de cómputo y móviles institucionales asignados.

9. POLÍTICA PARA USO DE CONEXIONES REMOTAS

El BOSTON INTERNATIONAL SCHOOL establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la institución; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

Normas para uso de conexiones remotas

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la institución.

La Dirección de Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

La Dirección de Tecnología debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la institución de manera permanente.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la institución y deben acatar las condiciones de uso establecidas para dichas conexiones.

Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.

9 POLÍTICAS DE SEGURIDAD DEL PERSONAL

9.1 POLÍTICA RELACIONADA CON LA VINCULACIÓN DE FUNCIONARIOS

El BOSTON INTERNATIONAL SCHOOL reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizara siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

Normas relacionadas con la vinculación de Administrativos y docentes

Normas dirigidas a: Recursos Humanos

El Grupo de Recursos Humanos debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en la institución, antes de su vinculación definitiva.

El Grupo de Recursos Humanos debe certificar que los funcionarios de la institución firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo.

Normas dirigidas a: DIRECCIÓN, SUPERVISORES DE CONTRATO,

Debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de la institución.

Normas dirigidas a: PERSONAL PROVISTOS POR TERCERAS PARTES

El personal provisto por terceras partes que realicen labores en o para el BOSTON INTERNATIONAL SCHOOL, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

El personal provisto por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad de la Información del instituto.

POLÍTICA APLICABLE DURANTE LA VINCULACION DE FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

El BOSTON INTERNATIONAL SCHOOL en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Dirección en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan las Políticas de seguridad de la información de la institucion.

Toda la comunidad BOSTON INTERNATIONAL SCHOOL debe ser cuidadosa de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad.

Normas aplicables durante la vinculación de funcionarios y personal provisto por terceros

Normas dirigidas a: DIRECCION

La Dirección debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer el institucion

La Dirección debe promover la importancia de la seguridad de la información entre los miembros del cuerpo administrativo de la Institución y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de

las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.

La Dirección debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente de la institución, el tratamiento de las faltas de cumplimiento a las políticas de seguridad o los incidentes de seguridad que lo ameriten.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

Debe diseñar y ejecutar de manera permanente un programa de concienciación en seguridad de la información, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento de la misma.

Capacitar y entrenar a los funcionarios de la institución en el programa de concienciación en seguridad de la información para evitar posibles riesgos de seguridad.

Normas dirigidas a: CONSEJO DIRECTIVO

Debe aplicar el proceso disciplinario de la institución cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad de la información.

Normas dirigidas a: RECURSOS HUMANOS

El Grupo de Recursos Humanos debe convocar a los adminiatrativos y docentes a las charlas y eventos programados como parte del programa de concienciación en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

Normas dirigidas a: TODOS LOS USUARIOS

Admistrativos, docentes y diferentes daparatmentos y personal provisto por terceras partes que por sus funciones hagan uso de la información del BOSTON

INTERNATIONAL SCHOOL, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

10. POLÍTICA DE DESVINCULACIÓN, LICENCIAS, VACACIONES O CAMBIO DE LABORES DE LOS FUNCIONARIOS Y PERSONAL PROVISTO POR TERCEROS

El BOSTON INTERNATIONAL SCHOOL asegurará que su cuerpo administrativo, docentes, diferentes departamentos y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros

Normas dirigidas a: RECURSOS HUMANOS

El Grupo de Recursos Humanos debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios del instituto llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Normas dirigidas a: DIRECCIÓN, SUPERVISORES DE CONTRATO

Debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a la Recursos Humanos.

Normas dirigidas a: RECURSOS HUMANOS

Debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe solicitar la modificación o inhabilitación de usuarios a la Dirección de Tecnología.

11.POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

POLÍTICA DE RESPONSABILIDAD POR LOS ACTIVOS

El BOSTON INTERNATIONAL SCHOOL como propietario de la información física así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad del BOSTON INTERNATIONAL SCHOOL, son activos de la institución y se proporcionan a los administrativos, docentes, diferentes departamentos y terceros autorizados, para cumplir con los propósitos del proceso academico.

Toda la información sensible del BOSTON INTERNATIONAL SCHOOL, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte DIRECCION. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

Normas de responsabilidad por los activos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

DIRECTIVAS,CONSEJO ADMINITARTIVO, deben actuar como propietarias de la información física y electrónica de la entidad, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin

Los propietarios de los activos de información deben generar un inventario de dichos activos para las áreas o procesos que lideran, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.

Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.

Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la institución, se encuentran sujetos a auditorías por parte de recursos humanos y a revisiones de cumplimiento.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la institución y, en consecuencia, debe asegurar su apropiada operación y administración.

La Dirección de Tecnología, son quienes deben autorizar la instalación, cambio o eliminación de componentes de la plataforma tecnológica del BOSTON INTERNATIONAL SCHOOL.

La Dirección de Tecnología debe establecer una configuración adecuada para los recursos tecnológicos, con el fin de preservar la seguridad de la información y hacer un uso adecuado de ellos.

La Dirección de Tecnología es responsable de preparar las estaciones de trabajo fijas y/o portátiles de los funcionarios y de hacer entrega de las mismas.

SEGURIDAD Y SALUD EN EL TRABAJO

El departamento de seguridad y salud en el trabajo debe realizar un análisis de riesgos de seguridad de manera periódica, sobre los procesos de la institución.

El departamento de seguridad y salud en el trabajo debe definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

El departamento de seguridad y salud en el trabajo debe realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información del instituto.

Normas dirigidas a: DIRECCIÓN Y JEFES DE DEPARTAMENTO

DIRECCIÓN Y JEFES DE DEPARTAMENTO, o quien ellos designen, deben autorizar a sus funcionarios el uso de los recursos tecnológicos, previamente preparados por la Dirección de Tecnología.

DIRECCIÓN Y JEFES DE DEPARTAMENTO, o quien ellos designen, deben recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran del instituto o son trasladados de área.

Normas dirigidas a: TODOS LOS USUARIOS

Los recursos tecnológicos del BOSTON INTERNATIONAL SCHOOL, deben ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes, con el fin de evitar daños o pérdidas sobre la operación o la imagen de la institución.

Los recursos tecnológicos del BOSTON INTERNATIONAL SCHOOL asignados a su cuerpo Administrativo, docentes, diferentes dapartamentos y personal suministrado por terceras partes, son proporcionados con el único fin de llevar a cabo las labores de la institucion; por consiguiente, no deben ser utilizados para fines personales o ajenos a estas.

EL cuerpo Administrativo, docentes, diferentes departamentos no deben utilizar software no autorizado o de su propiedad en la plataforma tecnológica del BOSTON INTERNATIONAL SCHOOL.

Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo a TALENTO HUMANO o quien este delegue; así

mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

12. POLÍTICA DE CLASIFICACIÓN Y MANEJO DE LA INFORMACIÓN

El BOSTON INTERNATIONAL SCHOOL definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información del BOSTON INTERNATIONAL SCHOOL debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por el Departamento de Sistemas y dirección.

Una vez clasificada la información, el BOSTON INTERNATIONAL SCHOOL proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de la comunidad boston de la institucion y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

Normas para la clasificación y manejo de la información

Normas dirigidas a: DEPARTAMENTO DE SISTEMAS DE INFORMACION Y TECNOLOGIA

El DEPARTAMENTO DE SISTEMAS DE INFORMACION Y TECNOLOGIA debe recomendar los niveles de clasificación de la información propuestos por el Departamento de SEGURIDAD Y SALUD EN EL TRABAJO y la guía de clasificación de la Información de la intitucion para que sean aprobados por la Junta Directiva.

Normas dirigidas a: SEGURIDAD Y SALUD EN EL TRABAJO

Debe definir los niveles de clasificación de la información para la institución y, posteriormente generar la guía de clasificación de la información.

EL DEPARTAMENTO SEGURIDAD Y SALUD EN EL TRABAJO debe socializar y divulgar la guía de clasificación de la Información a los funcionarios del instituto.

EL DEPARTAMENTO SEGURIDAD Y SALUD EN EL TRABAJO debe monitorear con una periodicidad establecida la aplicación de la guía de clasificación de la Información.

Normas dirigidas a: DEPARTAMENTO DE SISTEMAS DE INFORMACION Y TECNOLOGIA

DEPARTAMENTO DE SISTEMAS DE INFORMACION Y TECNOLOGIA debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.

DEPARTAMENTO DE SISTEMAS DE INFORMACION Y TECNOLOGIA debe efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: DEPARTAMENTO DE SISTEMAS DE INFORMACION Y TECNOLOGIA Y SEGURIDAD Y SALUD EN EL TRABAJO

Deben definir los métodos de cifrado de la información de la Entidad de acuerdo al nivel de clasificación de los activos.

Normas dirigidas a:DEPARTAMENTO DE SISTEMAS DE INFORMACION Y TECNOLOGIA Y SEGURIDAD Y SALUD EN EL TRABAJO

Debe utilizar los medios de los cuales está dotada para destruir o desechar correctamente la documentación física, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.

Debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

La Coordinación de Archivo debe verificar el cumplimiento de los Acuerdos de Niveles de Servicio y Acuerdos de intercambio con el proveedor de custodia externo de los medios de almacenamiento y documentos del instituto.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de los activos de información deben clasificar su información de acuerdo con la guías de clasificación de la Información establecida. Los propietarios de los activos de información son responsables de monitorear periódicamente la clasificación de sus activos de información y de ser necesario realizar su re-clasificación.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física institucional. La información física y digital del BOSTON INTERNATIONAL SCHOOL debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de expiración, toda la información debe ser eliminada adecuadamente. Los usuarios deben tener en cuenta estas consideraciones cuando imprimen, escanean, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada. Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación. La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

13. POLÍTICA DE USO DE PERIFERICOS Y MEDIOS DE ALMACENAMIENTO

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica del BOSTON INTERNATIONAL SCHOOL será reglamentado por la Dirección de Tecnología, junto con la SEGURIDAD Y SALUD EN EL TRABAJO, considerando las labores realizadas por los funcionarios y su necesidad de uso.

Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

La Dirección de Tecnología y la Oficina de Riesgos deben establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la institución.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica del instituto, de acuerdo con los lineamientos y condiciones establecidas.

La Dirección de Tecnología debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la institución, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

Normas dirigidas a: TODOS LOS USUARIOS

Administrativos, docentes y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.

Administrativos, docentes de la institución y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por la Dirección de Tecnología.

Administrativos, docentes de la institución y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados.

Administrativos, docentes de la institución y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales

Administrativos, docentes de la institución y personal provisto por terceras partes son responsables de la información institucional guardada en cada dispositivo asignado sincronizado en google drive (nube)

14. POLÍTICAS DE CONTROL DE ACCESO

14.1 POLÍTICA DE ACCESO A REDES Y RECURSOS DE RED

El departamento de sistemas de información y tecnología , como responsables de las redes de datos y los recursos de red de la institución, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Normas de acceso a redes y recursos de red

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la intitucion

La Dirección de Tecnología debe asegurar que las redes inalámbricas de la institución cuenten con métodos de autenticación que eviten accesos no autorizados.

El departamento de sistemas de información y tecnología ,debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la institución, así como velar por la aceptación de las responsabilidades de dicho terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

El departamento de sistemas de información y tecnología ,debe autorizar la creación o modificación de las cuentas de acceso a las redes o recursos de red de la institución.

El departamento de sistemas de información y tecnología ,verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.

Normas dirigidas a: TODOS LOS USUARIOS

Administrativos, docentes y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la institución, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.

Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la institución deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

15. POLÍTICA DE ADMINISTRACIÓN DE ACCESO DE USUARIOS

El BOSTON INTERNATIONAL SCHOOL establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la institución. Así mismo, velará porque los administrativos, docentes y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la

asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

Normas de administración de acceso de usuarios

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la institución, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

La Dirección de Tecnología, previa solicitud de los Jefes de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de información como de los diferentes departamentos , debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

La Dirección de Tecnología, debe definir lineamientos para la configuración de contraseñas que aplicaran sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la intucion; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

La Dirección de Tecnología debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

La Dirección de Tecnología debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

Recursos humanos debe autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información del instituto.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

Normas dirigidas a: DIRECCIÓN, JEFES DE DEPARTAMENTO

Deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.

POLÍTICA DE RESPONSABILIDADES DE ACCESO DE LOS USUARIOS

Los usuarios de los recursos tecnológicos y los sistemas de información del BOSTON INTERNATIONAL SCHOOL realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la institución deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

Usuarios comunidad BOSTON no deben compartir sus cuentas de usuario y contraseñas con usuarios o con personal provisto por terceras partes.

Usuarios y personal provisto por terceras partes que posean acceso a las plataformas tecnológicas, los servicios de red y los sistemas de información del instituto deben acogerse a lineamientos para la configuración de contraseñas implantados por la institución.

15.1. POLÍTICA DE USO DE ALTOS PRIVILEGIOS Y UTILITARIOS DE ADMINISTRACION

La Dirección de Tecnología del BOSTON INTERNATIONAL SCHOOL velará porque los recursos de la plataforma tecnológica y los servicios de red del institucion sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.

Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a: DIRECCION DE TECNOLOGIA, ADMINISTRADORES DE LOS RECURSOS TECNOLÓGICOS Y SERVICIOS DE RED

La Dirección de Tecnología debe otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos usuarios designados para dichas funciones.

La Dirección de Tecnología debe establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

La Dirección de Tecnología debe verificar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.

La Dirección de Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

La Dirección de Tecnología debe asegurarse que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

La Dirección de Tecnología debe establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

Los administradores de los recursos tecnológicos y servicios de red, funcionarios de la Dirección de Tecnología, no deben hacer uso de los utilitarios que permiten acceso a los sistemas operativos, firmware o conexión a las bases de datos para pasar por alto la seguridad de los sistemas de información alojados sobre la plataforma tecnológica de la institucion.

Los administradores de los recursos tecnológicos deben deshabilitar las funcionalidades o servicios no utilizados de los sistemas operativos, el firmware y las bases de datos. Se debe configurar el conjunto mínimo requerido de funcionalidades, servicios y utilitarios.

La Dirección de Tecnología debe generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

15.2. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICATIVOS

La institución como propietaria de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.

La Dirección de Tecnología, como responsable de la administración de dichos sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, velará porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la institución.

La Dirección de Tecnología debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

La Dirección de Tecnología debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

La Dirección de Tecnología debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

La Dirección de Tecnología debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

Normas dirigidas a: DESARROLLADORES (INTERNOS Y EXTERNOS)

Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.

Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.

Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.

Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

Los desarrolladores deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.

Los desarrolladores deben asegurar que si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.

Los desarrolladores deben certificar que el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.

Los desarrolladores deben asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.

Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

Los desarrolladores deben establecer que periódicamente se re-valide la autorización de los usuarios en los aplicativos y se asegure que sus privilegios no han sido modificados.

16. POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL

POLÍTICA DE AREAS SEGURAS

El BOSTON INTERNATIONAL SCHOOL proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Normas de áreas seguras

Normas dirigidas a: DIRECCION DE TECNOLOGIA

Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la Dirección de Tecnología autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha dirección durante su visita al centro de cómputo o los centros de cableado.

La Dirección de Tecnología debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

La Dirección de Tecnología debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un usuario autorizado.

La Dirección de Tecnología debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.

La Dirección de Tecnología debe velar porque los recursos de la plataforma tecnológica de la institución ubicados en el centro de cómputo se encuentren protegidos contra fallas o interrupciones eléctricas.

La Dirección de Tecnología debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

La Dirección de Tecnología debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: ADMINISTRATIVOS DIRECTORES Y JEFES DE OFICINA

Los Administrativos, Directores y Jefes de Oficina que se encuentren en áreas restringidas deben velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su áreas.

Los administrativos, Directores y Jefes de Oficina que se encuentren en áreas restringidas deben autorizar cualquier ingreso temporal a sus áreas, evaluando la pertinencia del ingreso; así mismo, deben delegar en personal del área el registro y supervisión de cada ingreso a sus áreas.

Los administrtivos, Directores y Jefes de Oficina deben velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los funcionarios autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros funcionarios del instituto.

17. POLÍTICA DE SEGURIDAD PARA LOS EQUIPOS INSTITUCIONALES

El BOSTON INTERNATIONAL SCHOOL para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica del institución que se encuentren dentro de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Normas de seguridad para los equipos institucionales

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro de las instalaciones de la institución.

La Dirección de Tecnología debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la institución.

La Dirección de Tecnología, en conjunto con la Coordinación de Recursos Físicos debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

La Dirección de Tecnología debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios del instituto y configurar dichos equipos acogiendo los estándares generados.

La Dirección de Tecnología debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos del instituto y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

La Dirección de Tecnología debe aislar los equipos de áreas sensibles, como la Dirección de Tesorería para proteger su acceso de los demás funcionarios de la red de la empresa.

La Dirección de Tecnología debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios del instituto, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: RECURSOS HUMANOS

Tiene la responsabilidad de incluir dentro del plan anual de auditorías la verificación aleatoria a los equipos de cómputo de todas las dependencias y puntos de atención de la entidad.

Normas dirigidas a: OFICINA DE RIESGOS

La Oficina de Riesgos debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas del instituto, en particular de las áreas sensibles.

Normas dirigidas a: RECURSOS HUMANOS

Debe revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.

Recursos humanos debe restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.

Velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la institución cuente con la autorización documentada y aprobada previamente por el Coordinador.

Velar porque los equipos que se encuentran sujetos a traslados físicos fuera del instituto, posean pólizas de seguro.

Normas dirigidas a: TODOS LOS USUARIOS

La Dirección de Tecnología es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la institución.

Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los usuarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione la Dirección de Tecnología.

Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad del BOSTON INTERNATIONAL SCHOOL el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o

escalará al interior de la Dirección de Tecnología, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la institución, solo puede ser realizado por la Dirección de Tecnología, o personal de terceras partes autorizado por dicha dirección.

Los funcionarios de la institución y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos.

Los equipos de cómputo deben ser transportados en las instalaciones con las medidas de seguridad apropiadas, que garanticen su integridad física.

Está prohibido sacar los equipos de la institución.

En caso de pérdida o robo de un equipo de cómputo de la institución, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

Los usuarios de la institución y el personal provisto por terceras partes deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

Los usuarios de la institución y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

18. POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

POLÍTICA DE ASIGNACIÓN DE RESPONSABILIDADES OPERATIVAS

La Dirección de Tecnología, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de la institución , asignará funciones específicas a sus usuarios, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

La Dirección de Tecnología proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información del instituto, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

Normas de asignación de responsabilidades operativas

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica de la institución.

La Dirección de Tecnología debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la institución.

La Dirección de Tecnología debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de

compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

La Dirección de Tecnología, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Normas dirigidas a: OFICINA DE RIESGOS

La Oficina de Riesgos debe emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para la plataforma tecnológica del institución.

POLÍTICA DE PROTECCIÓN FRENTE A SOFTWARE MALICIOSO

El BOSTON INTERNATIONAL SCHOOL proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

Normas de protección frente a software malicioso

Normas dirigidas a: DIRECCIÓN DE TECNOLOGÍA

La Dirección de Tecnología debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la intitucion y los servicios que se ejecutan en la misma.

La Dirección de Tecnología debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

La Dirección de Tecnología debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

La Dirección de Tecnología, a través de la comunidad boston, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

La Dirección de Tecnología, a través de la comunidad boston, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios de recursos tecnológicos no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam definida por la Dirección de Tecnología; por consiguiente, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.

Los usuarios de recursos tecnológicos deben ejecutar el software de antivirus, antispyware, antispam, antimalware sobre los archivos y/o documentos que son abiertos o ejecutados por primera vez, especialmente los que se encuentran en medios de almacenamiento externos o que provienen del correo electrónico.

Los usuarios deben asegurarse que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Mesa de Ayuda, para que a través de ella, la Dirección de Tecnología tome las medidas de control correspondientes.

19. POLÍTICA DE COPIAS DE RESPALDO DE LA INFORMACIÓN

El BOSTON INTERNATIONAL SCHOOL certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades. Las áreas propietarias de la información, con el apoyo de la Dirección de Tecnología, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, la institución velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Normas de copias de respaldo de la información

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología, a través de sus usuarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

La Dirección de Tecnología debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

La Dirección de Tecnología, a través de sus usuarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

La Dirección de Tecnología debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de los activos de información de la institución.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con la Dirección de Tecnología, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: TODOS LOS USUARIOS

Es responsabilidad de los usuarios de la plataforma tecnológica del BOSTON INTERNATIONAL SCHOOL identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

POLÍTICA DE REGISTRO DE EVENTOS Y MONITOREO DE LOS RECURSOS TECNOLÓGICOS Y LOS SISTEMAS DE INFORMACIÓN

El BOSTON INTERNATIONAL SCHOOL realizará monitoreo permanente del uso que dan los usuarios y el personal provisto por terceras partes a los recursos de la plataforma tecnológica y los sistemas de información de la institución. Además, velará por la custodia de los registros de auditoría cumpliendo con los periodos de retención establecidos para dichos registros.

La Dirección de Tecnología y la Oficina de Riesgos definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos misionales del instituto. El Comité de revisión de logs mensualmente se reunirá para analizar los resultados del monitoreo efectuado.

POLÍTICA DE CONTROL AL SOFTWARE OPERATIVO

El BOSTON INTERNATIONAL SCHOOL, a través de la Dirección de Tecnología, designará responsables y establecerá procedimientos para controlar la instalación de software operativo, se cerciorará de contar con el soporte de los proveedores de dicho software y asegurará la funcionalidad de los sistemas de información que operan sobre la plataforma tecnológica cuando el software operativo es actualizado.

Normas de control al software operativo

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe establecer responsabilidades y procedimientos para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en el instituto.

La Dirección de Tecnología debe asegurarse que el software operativo instalado en la plataforma tecnológica de la institución cuenta con soporte de los proveedores.

La Dirección de Tecnología debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

La Dirección de Tecnología debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

La Dirección de Tecnología debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la institución .

POLÍTICA DE GESTIÓN DE VULNERABILIDADES

El BOSTON INTERNATIONAL SCHOOL, a través de la Dirección de Tecnología y la Oficina de Riesgos, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Estas dos áreas conforman el Comité de vulnerabilidades encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

Normas para la gestión de vulnerabilidades

Normas dirigidas a: OFICINA DE RIESGOS

La Oficina de Riesgos debe adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.

La Oficina de Riesgos debe generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.

La Dirección de Tecnología, a través de sus funcionarios, debe generar y ejecutar o monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y OFICINA DE RIESGOS

La Dirección de Tecnología y la Oficina de Riesgos, a través del Comité de vulnerabilidades, deben revisar, valorar y gestionar las vulnerabilidades técnicas encontradas, apoyándose en herramientas tecnológicas para su identificación.

20. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

POLÍTICA DE GESTION Y ASEGURAMIENTO DE LAS REDES DE DATOS

El BOSTON INTERNATIONAL SCHOOL establecerá, a través de la Dirección de Tecnología, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida del instituto.

Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la institución.

La Dirección de Tecnología debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos

La Dirección de Tecnología debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para la institución.

La Dirección de Tecnología debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

La Dirección de Tecnología debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la institución, acogiendo buenas prácticas de configuración segura.

La Dirección de Tecnología, a través de sus usuarios, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por el instituto en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

La Dirección de Tecnología debe instalar protección entre las redes internas de la institución y cualquier red externa, que esté fuera de la capacidad de control y administración del instituto.

La Dirección de Tecnología debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos de la institución.

POLÍTICA DE USO DEL CORREO ELECTRONICO

El BOSTON INTERNATIONAL SCHOOL, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre usuarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

Normas de uso del correo electrónico

Normas dirigidas a: DIRECCION DE TECNOLOGIA Y RECURSOS HUMANOS

La Dirección de Tecnología debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

La Dirección de Tecnología debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

La Dirección de Tecnología debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.

La Dirección de Tecnología debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

La Dirección de Tecnología, con el apoyo de RECURSOS HUMANOS, debe generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la institución o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional del BOSTON INTERNATIONAL SCHOOL. El correo institucional no debe ser utilizado para actividades personales.

Los mensajes y la información contenida en los buzones de correo son propiedad del BOSTON INTERNATIONAL SCHOOL y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

Los usuarios de correo electrónico institucional tienen prohibido el envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la institución y el personal provisto por terceras partes.

No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la institución y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

POLÍTICA DE USO ADECUADO DE INTERNET

El BOSTON INTERNATIONAL SCHOOL consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la institución.

Normas de uso adecuado de internet

Normas dirigidas a: DIRECCION DE TECNOLOGIA

La Dirección de Tecnología debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

La Dirección de Tecnología debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

La Dirección de Tecnología debe monitorear continuamente el canal o canales del servicio de Internet.

La Dirección de Tecnología debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

La Dirección de Tecnología debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Generar campañas para concientizar tanto a los usuarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

Los usuarios del servicio de Internet del BOSTON INTERNATIONAL SCHOOL deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del proceso aducativo

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la

integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

No está permitido el intercambio no autorizado de información de propiedad del BOSTON INTERNATIONAL SCHOOL, de sus clientes y/o de sus usuarios, con terceros.

POLÍTICA DE INTERCAMBIO DE INFORMACIÓN

El BOSTON INTERNATIONAL SCHOOL asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. La institución propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

Normas de intercambio de información

Normas dirigidas a: DIRECCIÓN – GRUPO DE CONTRATACIÓN

El Grupo de Contratación, en acompañamiento con la Oficina de Riesgos, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre el instituto y tercera partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la institución a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.

El Grupo de Contratación debe establecer en los contratos que se establezcan con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios del instituto que les ha sido entregada en razón del cumplimiento de los objetivos misionales de la institucion .

Controles físicos y ambientales

- Seguridad mediante personal
- Equipo informático en áreas de acceso controlado
- Vigilancia con video en toda la instalación y el perímetro
- Alimentación Principal eléctrica subterránea
- Sistemas de alimentación ininterrumpida (UPS)
- Hay extinguidores de incendio en todas las áreas

Controles de acceso lógico

Identificación de usuario y administración de accesos

EQUIPO DE COMPUTO

- Perfiles de administrador y usuario
- Contraseña administrador y usuario

REDES WIFI

Contraseñas

SOFTWARE

Software contable, matrículas y académico perfiles definidos y contraseña

- Administrador
- Director de area
- Usuario

Correo Electrónico GOOGLE APPS

- Contraseña personal
- Doble autenticación vía celular

PLATAFORMAS EXTERNAS

- Perfiles de usuario
- Administrador y usuario
- Contraseñas

Controles de seguridad opcionales

- Se conectan a Internet a través de distintos enlaces enrutados redundantes de varios proveedores de servicio de Internet abastecidos desde múltiples puntos de presencia de proveedores de telecomunicaciones
- UTM proporciona bloqueo de paginas restringidas, virus y control del tráfico
- Las copias de seguridad se guardan en google drive sincronizado en un disco duro de computador administrador

USUARIO REDBOSTON - LO QUE NUNCA SE DEBE HACER.

- No descargar musica, peliculas u otros archivos no legales
- No abrir documentos adjuntos o hacer click en enlaces no solicitados
- No visitar sitios web pornograficos o de contenido ilicito
- No proporcionar datos personales a desconocidos por teléfono o email
- No utilizar la misma contraseñas en correos, plataformas y páginas web O compartirlas

- Excesiva y abusiva navegación por internet con fines no laborales o no justificados por tarea
- Ocupación de memoria y demás recursos con fines personales
- Descarga ilegal de software no licenciado
- Descarga ilegal de música
- Trafico de material pornografico, violento y con fines no éticos
- Uso del correo para fines personales
- Transmisión a terceros de información confidencial
- Inutilización de sistemas y equipos informáticos

Aviso de Privacidad

"Por este medio acepto plenamente y autorizo a la INSTITUCIÓN EDUCATIVA COLEGIO BOSTON INTERNATIONAL a la recolección y tratamiento de los datos personales a través de formularios físicos, electrónicos o por cualquier medio por el cual pueda entregar a la INSTITUCIÓN EDUCATIVA información personal, para que esta proceda con la incorporación de los datos facilitados en la bases de datos de las cuales es titular y responsable la INSTITUCIÓN EDUCATIVA, y su tratamiento en los términos estipulados en el presente documento y en las normas vigentes al interior de la INSTITUCIÓN EDUCATIVA. La finalidad para la recolección, uso y tratamiento de datos personales a que se refiere esta política es la adecuada gestión, administración, mejora de las actividades y distintos servicios de la INSTITUCIÓN EDUCATIVA, realización de procesos internos, estadísticas, análisis cuantitativo y cualitativo de las actividades, tales como uso del campus o de los servicios ofrecidos por la INSTITUCIÓN EDUCATIVA, entre otros que resulten de interés para la institución. Igualmente podrá referirse al ofrecimiento de nuevos productos o mejora de los existentes que puedan contribuir con el bienestar académico, administrativo, financiero o de formación, ofrecidos por la INSTITUCIÓN EDUCATIVA o por terceros relacionados con su objeto. Manifiesto que la información anteriormente entregada a la INSTITUCIÓN EDUCATIVA es totalmente actual, exacta y veraz y reconozco mi obligación de mantener, en todo momento, actualizados los datos, de forma tal que sean veraces y exactos. En todo caso, reconozco que soy el único responsable de la información falsa o inexacta que realice y de los perjuicios que cause a la INSTITUCIÓN EDUCATIVA o a terceros, por la información que facilite.
Al facilitar datos de carácter personal, acepto igualmente la remisión de información acerca de noticias, cursos, eventos, boletines y productos relacionados con la INSTITUCIÓN EDUCATIVA. La INSTITUCIÓN EDUCATIVA hará un uso responsable de la información entregada por los titulares, además de lo consagrado en su política de privacidad de uso y tratamiento de información personal, privacidad y confidencialidad de la información existente en las bases de datos sólo suministrará información cuando este lo solicite o autorice expresamente, cuando medie decisión judicial o administrativa o cuando esta información esté prevista en los convenios interinstitucionales suscritos por la INSTITUCIÓN EDUCATIVA.
He sido informado sobre el carácter facultativo que tiene el suministro de información sensible la cual tendrá carácter reservado y acerca de los derechos que me asisten como titular, para conocer, actualizar y solicitar la rectificación o supresión de datos conforme a los procedimientos y políticas de la institución establecidas en: www.redboston.edu.co Así mismo, que no estoy obligado a autorizar el tratamiento de datos con naturaleza sensible. La responsabilidad en el tratamiento de la presente información estará a cargo del COLEGIO BOSTON INTERNACIONAL Calle 74 41-46 Barranquilla- Colombia - Tel. (57) (605) 3225296 - Barranquilla, Colombia.