ISEA
La Escuela en su Casa

Instituto Superior de Educación Abierta

21 Av. 33-58 Zona 12 Santa Elisa. PBX 2387-3100 www.isea.edu.gt

Al que cree, todo le es posible. Marcos 9:23

Políticas de Seguridad Digital

Definición.

A lo largo de este documento se utiliza el término escuela, la escuela, esta escuela o ISEA. En estos casos nos estamos refiriendo al Instituto Superior de Educación Abierta – ISEA - .

Introducción.

Este manual de políticas de seguridad es un conjunto de estrategias y normas que deben ser observadas por todas aquellas personas a quienes se les da acceso a las plataformas tecnológicas, correos electrónicos, equipos y cualquier otro dispositivo pertenezca uno a esta escuela pero que se utiliza para acceder a los diferentes servicios digitales de los que esta escuela dispone.

Estas políticas de seguridad tienen el propósito de informar a todos los usuarios, sean estos personal docente o administrativo, estudiantes, padres de familia y cualquier otra persona que por cualquier motivo necesita acceder a los sistemas o equipos pertenecientes a la escuela; de sus obligaciones, requerimientos para proteger la tecnología e información de todos los usuarios.

Estas políticas de seguridad describen los dispositivos, la tecnología y plataformas que debemos proteger e identifica alguno de los riesgos relacionados a los mismos.

Estas políticas de seguridad también describen las responsabilidades y privilegios de cada usuario. ¿Qué se considera uno su aceptable? ¿Cuáles son las normas concernientes al acceso al Internet dentro de las instalaciones de la escuela? Este manual de políticas responde a estas preguntas, describen las limitaciones de los usuarios e informa acerca de las penalizaciones por la violación de estas políticas. Este documento también contiene procedimientos para responder a incidentes que ponen en riesgo la seguridad del equipo o plataformas de la escuela, pero más importante aún la seguridad física o emocional de los estudiantes.

¿Qué estamos protegiendo?

Es obligación de todos los usuarios de los sistemas de la escuela, proteger la tecnología y la información existente en cada una de las plataformas o equipos. Esta información debe ser protegida contra el uso no autorizado de la misma, el acceso sin permiso, el robo o la destrucción. Los recursos tecnológicos de la escuela son compuestos de la siguiente lista la cual no debe ser tomada como definitiva:

1. Equipos de computación, CPU, discos, correos electrónicos, aplicaciones web, servidores, dispositivos móviles, aplicaciones de software, etc.
2. Sistemas de software que incluye, sistemas operativos, bases de datos, aulas virtuales (Canvas LMS), sistemas de restauración o de respaldo, sistemas de comunicación, etc.
3. Software específico utilizado por departamentos tales como recursos humanos, contabilidad, tutoría y otros. Esto incluye cualquier código escrito exclusivamente para esta escuela y el uso comercial de paquetes de suscripción tales como ofimática, mensajería, supervisión y otros.
4. Redes de comunicación tanto físicas como digitales; incluyendo routers, racks, cables, antenas, hubs, firewalls, líneas privadas y cualquier herramienta similar.

Contenido

Clasificación de la información.

Toda información de los usuarios que se almacena en archivos locales o en la nube, así como bases de datos deben ser clasificados como confidenciales o no confidenciales. La escuela clasificará la información controlada por cada departamento. El gerente de tecnología o quien realice sus funciones tiene la obligación de revisar y aprobar la clasificación de la información y determinar el nivel apropiado de seguridad para protegerlo. Asimismo, esta persona deberá aprobar la clasificación de la información controlada por entidades ajenas a esta escuela, pero cuyos servicios son utilizados bajo sistema de suscripción o contrato.

Nivel de seguridad	Descripción	¿Qué servicios tienen este nivel?
ROJO	Este sistema contiene toda la información confidencial que no puede ser revelada a personas que no pertenecen a esta escuela. Incluso dentro de la escuela, el acceso a esta información debe ser provisto sobre la base de la “necesidad de saberlo”. El sistema provee servicios críticos para la operación de la escuela, la omisión de estas políticas traerá graves consecuencias e impactará de forma adversa la operación de la escuela, el bienestar de los alumnos y demás miembros de la comunidad educativa.	Servidor SIS (Student Information System) en donde se almacena todos los datos de los estudiantes, incluyendo nombres, direcciones de casa, números de teléfono y correos electrónicos entre otros. Canvas LMS Aula Virtual donde se lleva todo el proceso de enseñanza y aprendizaje.

VERDE	Este sistema no contiene información confidencial ni depende de servicios críticos, pero provee la habilidad para acceder a los sistemas rojos a través de la red interna o externa.	Equipos de computación propios de la escuela, servidores en la nube e información que puede compartirse con terceras personas tales como Slack o JivoChat.
BLANCO	Estos son aquellos sistemas que no están accesibles desde fuera. No es posible acceder a ellos a través de una red normal y no contiene o ejecuta información sensitiva.	Documentos guardados con soporte de papel tales como certificados y diplomas emitidos por el Ministerio de Educación.
NEGRO	Este es un sistema accesible desde fuera; está aislado de cualquier elemento rojo o verde por medio de un muro de fuego (Firewall). Y aunque ejecuta servicios importantes no contiene información confidencial.	Página web

Esta es una lista bastante limitada y podrá cambiar en cualquier momento sin previo aviso.

Redes locales (LAN)

Todas las redes locales en esta escuela son accesibles únicamente desde dentro de las instalaciones a través de un sistema de cableado RJ45.

Riesgos de seguridad.

Personal docente, administrativo y estudiantes.

1. Cada profesor, tutor o personal administrativo y estudiantes inscritos en esta escuela recibirá un correo electrónico administrado por Google con la terminación @isea.edu.gt que les permitirá el acceso a los servicios de correo electrónico, aula virtual, Secretaría virtual. Cada individuo es responsable del uso que al usuario y contraseña asignado.
2. Dependiendo del rol asignado, los diferentes sistemas darán acceso a los distintos módulos que componen cada una de las plataformas.
3. En el evento de extraviar la contraseña, divulgarla por cualquier medio o comprometerla de otra forma, deberá avisar inmediatamente al correo electrónico soporte@isea.edu.gt para que le sea aceptada una nueva contraseña. No dar aviso, o en su defecto, si alguien tiene acceso a las credenciales aún con el desconocimiento del respectivo usuario constituir una falta que podrá ser sancionada con una llamada de atención por escrito si el usuario es empleado directo de esta escuela.
4. En el caso de los estudiantes, se dará aviso inmediato a los padres de familia o encargados para que ellos tomen las precauciones necesarias. No puede ser penalizado cualquier estudiante que por descuido extravíe o comparta sus datos, sin embargo, no podrá alegar a su favor la pérdida de las credenciales para obtener algún beneficio en sus calificaciones.

5. En el evento de que un empleado se ha suspendido de sus labores o despedido definitivamente, el gerente de soporte o la persona que haga sus funciones deberá bloquear inmediatamente los equipos y cuentas o correos electrónicos asignados a tal persona.
6. Cuando un estudiante se retira de esta escuela por transferencia a otra, por haber finalizado los estudios o por abandono de estos, su correo electrónico no será deshabilitado siempre y cuando se mantenga activo. Los correos podrán ser deshabilitados cuando los usuarios no hayan accedido a los mismos por más de seis meses.
7. Todos los equipos que pertenecen a esta escuela y que se encuentran instalados en cualquiera de las oficinas de esta, deben estar protegidos contra robo, contra cualquier calamidad o inclemencia y también protegidos por posibles sobrecargas o pérdida de corriente eléctrica.

Hackers o vandalismo

1. Para asegurar todos los equipos pertenecientes a esta escuela contra cualquier hacker o vándalo que utilizando algún acceso a través del Internet quiera provocar daños a los sistemas internos, se debe activar en todas las computadoras o dispositivos un sistema de seguridad antivirus.
2. De la misma forma, para asegurar que los empleados utilizan los equipos y accesos de forma apropiada todos los equipos pertenecientes a esta escuela deberán tener instalado el software Time Doctor, que lleva el control del uso del teclado, de los accesos a todos los sitios, del tiempo que se le dedica a cada tarea y los proyectos asignados entre otros.
3. Cada sistema que está alojado en servidores en la nube debe contar obligatoriamente con un sistema de restauración en caso de pérdida de la información o el daño y manipulación por cualquier pirata informático.
4. Cuando se está trabajando, utilizando cualquiera de los equipos y/o plataformas se debe tener especial cuidado en no insertar contraseñas débiles y también tener mucho cuidado al hacerlo frente a usuarios con el fin de que estos no puedan detectar qué es lo que se está escribiendo.

Uso aceptable del equipo y plataformas.

1. El uso aceptable de las cuentas, de los equipos y de los demás sistemas utilizados en esta escuela debe ser única y exclusivamente para asuntos relativos al trabajo en el caso de los colaboradores directos de esta escuela o para los estudios en el caso de los estudiantes inscritos durante el ciclo escolar activo.
2. El uso de los equipos o sistemas de la escuela para fines personales o para dar servicio a otras empresas constituye un robo y violación a la propiedad intelectual no tangible castigado bajo las leyes de la República de Guatemala.
3. Cada usuario es responsable personalmente de proteger toda la información a la que tiene acceso dependiendo del rol de su respectiva cuenta. Esto incluye los usuarios y contraseñas, las direcciones electrónicas que no pueden ser divulgadas, y se les prohíbe terminantemente hacer copias no autorizadas de esa información o distribuirla fuera de la escuela.
4. Ningún usuario, se ha empleado o estudiante de esta escuela, en ninguna circunstancia jamás deberá intentar acosar, denigrar u obligar a otra persona especialmente los estudiantes a hacer cosas consideradas ilegales por las leyes guatemaltecas o internacionales. En el evento de

encontrarse a alguna persona que tiene relación de dependencia o es empleado o empleada de esta escuela, cometiendo cualquiera de los delitos anteriores o similares será despedido o despedida inmediatamente y denunciadas ante las autoridades judiciales de la República.

5. Ningún usuario tiene permiso para conectar dispositivos no autorizados a sus estaciones de trabajo a menos que hayan recibido autorización específica del gerente de tecnología o la persona que realice sus funciones.
6. Los usuarios no pueden descargar software no autorizado e instalar los en su computadora, así como tampoco está permitido descargar propiedad intelectual ajena tales como películas, vídeos, archivos PDF, etc. etc.; de los cuales la escuela no tenga licencia de uso.
7. Las plataformas de proveedores de contenido tales como BrainPOP, H5P y similares tampoco podrán ser utilizadas para fines distintos a los que han sido designados y no se puede compartir códigos o enlaces con personas ajenas a la escuela.
8. Todos los usuarios tienen la obligación de reportar cualquier riesgo que pueda existir por el uso o diseño de los sistemas o equipos pertenecientes a esta escuela.
9. La escuela provee acceso al Internet a todos los empleados y contratistas cuando se encuentren laborando dentro de las instalaciones, cualquier incidente o mal uso constituye una violación a la propiedad de esta escuela.
10. Los empleados y contratistas deben obtener permiso y solicitar las respectivas contraseñas a la gerencia de tecnología. El Internet es una herramienta de la escuela, se debe utilizar únicamente para asuntos relativos a las labores que se desarrollan dentro o fuera de las mismas tales como revisar contenidos en línea, acceder a sitios de información o plataformas de las cuales la escuela tiene licencia y para obtener información sobre los estudiantes entre otras cosas.
11. El servicio de Internet no puede ser utilizado para transmitir, descargar o almacenar cualquier texto, imagen o vídeo que sea discriminatorio o que sirva para acosar a estudiantes y demás empleados de esta escuela.
12. Los sistemas, plataformas, equipos o cualquier otro dispositivo propiedad de la escuela no podrán ser utilizados para acosar, discriminar a cualquier persona por su raza, situación socioeconómica, género, religión o preferencias sexuales.
13. En ninguna circunstancia se tolerará compartir “memes” o contenido multimedia que denigre a cualquier individuo bajo las circunstancias anteriores.

Clasificación de usuarios.

Categoría	Privilegios y responsabilidades
Administradores de sistema	Gerente de tecnología o cualquier persona que cumple las funciones de este puesto, tiene acceso administrativo o de superusuario a los servidores, plataformas tales como aula virtual, Secretaría virtual, sistema de chat, redes sociales, servidores en la nube, etc. Es el responsable final del buen manejo de toda la información, la categoría de la información que maneja es ROJO y no deberá ser compartida con ninguna persona dentro o fuera del establecimiento a menos que sea absolutamente necesario.
Usuarios administradores	En cada plataforma, tales como Canvas LMS, JivoChat, Secretaría Virtual, OpenSIS, Google Suite y SIRE (Ministerio de Educación) los usuarios administradores son las personas responsables de cada una de las plataformas y tienen acceso para poder administrar la información, crear usuarios, recuperar contraseñas, inscribir estudiantes, generar cuadros de calificaciones, certificados y diplomas entre otras cosas. La información que manejan es confidencial ROJO y sólo se le debe dar acceso a aquellas personas que han sido designadas para formar parte del departamento específico. Los usuarios administradores son los responsables de capacitar a todas aquellas personas bajo su departamento.
Usuarios internos.	Entendemos por usuario interno toda aquella persona que no tiene a su cargo un departamento pero que labora en el mismo, por lo tanto, tiene acceso a una o más áreas plataformas para realizar su trabajo. En esta categoría se encuentran principalmente los profesores, tutores, personal de Secretaría, atención al cliente, planta, etc.
Estudiantes y padres de familia.	Los estudiantes y padres de familia acceden a las distintas plataformas utilizando un usuario limitado, en el caso de los alumnos pueden acceder al aula virtual y poder trabajar utilizando únicamente su usuario, pero no tienen acceso a los demás cursos y no pueden ver la información de los compañeros que no pertenezca a su grado. Los padres de familia participan como observadores y pueden acceder también al aula virtual, Secretaría virtual, sistemas de

	pago o sistemas de información del estudiante OpenSIS utilizando el sistema de **Google Single Sign On SSO** que les confiere ciertos privilegios e información limitada.
Contratistas	Los contratistas son personas o empresas que trabajan sobre la base de un contrato y que les concede acceso a diferentes áreas de la escuela, las plataformas o equipos por un período de tiempo mientras se completa el proyecto para el cual han sido contratados. Dependiendo del tipo de proyecto los accesos pueden ser confidenciales o no y debe definirse claramente en el contrato de trabajo. Una vez finalizado el contrato y recibido a conformidad del producto los accesos deberán ser eliminados.
Público en general	el público en general puede tener acceso a todas aquellas páginas web de información general en donde se detallan los requisitos para ingresar a estudiar, información compartida en las redes sociales etc. El público tiene un acceso totalmente limitado a la información que existe en las plataformas, más allá de la información en las portadas o las instrucciones sobre cómo utilizar una u otra plataforma, así como tutoriales, materiales liberados bajo licencia Creative Commons entre otros.

Monitoreo del uso de computadoras y plataformas de la escuela.

1. La escuela se reserva el derecho de monitorear por cualquier medio todo equipo perteneciente a esta misma escuela o plataforma digital en propiedad o adquirida bajo un sistema de licencia.
2. En monitoreo se extiende también a todas las actividades realizadas dentro fuera de la escuela con el equipo o sistemas de su propiedad, incluyendo, pero no limitándose al correo electrónico, aplicaciones de ofimática, aulas virtuales etc. etc.
3. El software Time Doctor instalado en todos los equipos o dispositivos propiedad de esta escuela lleva un control exhaustivo de todos los sitios web visitados, el tiempo permanecido en los mismos, el uso del teclado, la introducción de contraseñas, y toda la actividad desarrollada en los horarios de trabajo.
4. Los tutores que laboran desde casa y que utilizan equipo propio no están obligados a instalar esta aplicación ni ninguna otra que controle lo que hacen con su equipo; sin embargo, al acceder a las plataformas digitales se guarda un historial del trabajo que hayan realizado en ellas.
5. La gerencia de tecnología es la encargada de asegurar que cada una de estas aplicaciones mantengan el historial de acciones realizadas por cada usuario. (log).

6. Las contraseñas no deberán ser fáciles de adivinar, los sistemas deberán configurarse de manera que cada usuario establezca su propia contraseña utilizando letras mayúsculas y minúsculas, números y símbolos.
7. Las contraseñas no deberán ser publicadas en ningún tipo de comunicación digital, y tampoco deberán ser escritas en papel ni colocadas cerca de las computadoras o estaciones de trabajo.
8. Las contraseñas deben ser cambiadas como mínimo a cada 90 días.
9. Los usuarios que no hayan accedido por más de 180 días o que no hayan utilizado su correo electrónico en esa misma cantidad de tiempo serán deshabilitados y deberán pasar el proceso completo de inscripción o contratación para reactivarlos de ser necesario.
10. Ningún usuario excepto personal administrativo de la gerencia de tecnología debe o puede tener acceso a los archivos que guardan las contraseñas de todos los usuarios.
11. Ningún usuario puede acceder como administrador a los equipos o dispositivos propiedad de la escuela excepto personal de la gerencia de tecnología.
12. Los usuarios de los empleados que cesen relación laboral con la escuela deberán ser desactivados el mismo día que la persona finaliza sus labores y se retira definitivamente.
13. Es responsabilidad de los supervisores de cada departamento dar aviso a la gerencia de tecnología para el traslado de toda la información y el formateo de los equipos respectivos.
14. Cuando algún usuario olvide su contraseña deberá ponerse en contacto al departamento de soporte o a la gerencia de tecnología para recuperarla.
15. Por políticas de Google las contraseñas de la aplicación Google Suite sólo puede ser recuperadas por el administrador del sistema.

Procedimientos para el manejo de incidentes de seguridad.

Un incidente de seguridad se define como cualquier situación irregular o adversa que pone en riesgo la seguridad, la integridad o disponibilidad de la información digital, así como la integridad física de los usuarios sean estos alumnos, padres de familia o empleados de la escuela.

Nivel de seguridad	Descripción	
ROJO	Cualquier violación de seguridad o riesgo a cualquier tipo de información o sistema marcado con el color rojo debe ser considerado como crítico y urgente por lo tanto se debe dar aviso por cualquier persona que lo haya detectado directamente al gerente de tecnología o la persona que realice sus funciones. Inmediatamente después deberá avisarse a las autoridades administrativas de la escuela.	Benjamín Ramirez Jorge.ramirez@isea.edu.gt

	Por tratarse de una situación de emergencia se debe procurar dar aviso verbal o por medio del teléfono inmediatamente.	
VERDE BLANCO NEGRO	Cualquier violación de seguridad o riesgo marcado con el color verde, blanco o negro debe ser informado inmediatamente al encargado o encargada del departamento o sede respectiva. Si esta persona no está disponible o después de habérsele avisado no hizo nada se debe entonces avisar directamente a la gerencia de tecnología o a la dirección administrativa.	Clarissa Noriega Clarissa.noriega@isea.edu.gt

Cualquier persona que habiéndose dado cuenta de cualquier riesgo violación a cualquiera de estos niveles de seguridad y no tiene aviso a las autoridades respectivas puede ser motivo de sanción incluyendo el despido si se trata de empleados de la escuela o el aviso a los respectivos padres de familia si fueran estudiantes.

Ningún estudiante puede ser sancionado castigado por no dar aviso de cualquiera de estas violaciones de seguridad ya que al ser menores de edad no puede ser imputados de ningún delito o falta.